IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, v. MOHAMMED AZHARUDDIN CHHIPA, *Defendant*.	Case No.: 1:23-cr-97 (DJN)

DEFENDANT'S MOTION TO SUPPRESS THE CONTENT OF UNLAWFUL ELECTRONIC SURVEILLANCE AND THE FRUIT THEREOF, AND TO COMPEL DISCLOSURE OF ALL SURVEILLANCE MATERIAL

Jessica N. Carmichael, VSB #78339
Zachary A. Deubler, VSB #90669
CARMICHAEL ELLIS & BROCK, PLLC
108 N. Alfred Street, 1st Floor
Alexandria, VA 22314
703.684.7908 (T)
703.649.6360 (F)
zach@carmichaellegal.com
jessica@carmichaellegal.com

Counsel for Mohammed Chhipa

TABLE OF CONTENTS

Mohammed Chhipa, by counsel, moves this Court: (1) to suppress all interceptions made and electronic surveillance and physical searches conducted under the Foreign Intelligence Surveillance Act (hereinafter "FISA"), 50 U.S.C. §1801, et seq., and any fruits thereof; (2) to suppress all material and any fruits thereof collected under the FISA Amendments Act (hereinafter "FAA" or "Section 702"), 50 U.S.C. §1881a, et seq., which undoubtedly occurred in this case; and (3) for disclosure of the underlying applications for FISA warrants, all Section 702 material including querying information, and all information on other government surveillance programs used to collect Mr. Chhipa's information. An evidentiary hearing is requested on these matters.

Suppression is required because the surveillance violated Mr. Chhipa's Constitutional protections. However, the details and specifics of these violations are currently unknowable. Disclosure of the FISA applications, Section 702 material, and other surveillance tools to defense counsel – who possess the requisite security clearances – is critical for Mr. Chhipa to develop his challenges to the legality of the surveillance fully and is required under the statutes and Constitution. This motion articulates the grounds for each relief requested to the extent possible on the limited information. Upon disclosure of additional requested material, Mr. Chhipa asks for leave to supplement or file additional motions.

BACKGROUND

Mohammed Chhipa is charged in a five-count Indictment with Conspiracy to Provide Material Support to a Foreign Terrorist Organization, in violation of 18

U.S.C. § 2339B (Count One); and Material Support of a Foreign Terrorist Organization in violation of 18 U.S.C. § 2339B (Counts Two through Five).

He was born in India and moved to the United States when he was four. Since then, he has lived, attended school, and worked in the Northern Virginia area. He has no criminal record. In fact, at one point, the FBI approached him to ask him to be an undercover informant, but he declined. At the time of Mr. Chhipa's arrest, he was working in Information Technology and supporting his parents with whom he lived. He was also trying to gain custody of his children, who are now in foster care, through the Loudoun County Court system.

The charges in this case stem from allegations that Mr. Chhipa collected and sent money to female Islamic State of Iraq and al-Sham (ISIS) members in Syria to benefit ISIS, which was and is a designated Foreign Terrorist Organization. The Indictment alleges that in 2021 and 2022, Mr. Chhipa sent a total of $840.00 to Unindicted Co-Conspirator 1 (UCC-1), who was a British-born ISIS member residing in Syria. The government alleges that these transactions were to support ISIS.

Mr. Chippa now moves for suppression of any and all evidence obtained pursuant to the FISA electronic surveillance and physical searches, and Section 702, as well as disclosure of the underlying applications for FISA warrants, Section 702 material, and notice of all other surveillance programs used.

ARGUMENT

On August 18, 2023, the government filed a notice stating that it intends to offer into evidence "to offer into evidence, or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained or derived from electronic surveillance and physical search conducted under the Foreign Intelligence Surveillance Act of 1978 (FISA)." ECF No. 50. The government has not provided notice of Section 702 collection on Mr. Chhipa, however, the timing of materials generated in this case, the facts alleged, the wording in the reports legal processes, and other known information about the procedures used by the FBI when opening a national security investigation indicates that Section 702 surveillance on Mr. Chhipa was collected and queried.

As detailed below, the material the government obtained under FISA and Section 702 and any other surveillance program should be suppressed because the surveillance and collection were conducted in violation of FISA and the First and Fourth Amendments. However, because defense counsel has not been provided with the underlying applications for the pertinent FISA warrants, the 702 material, and all the surveillance programs involved in collecting Mr. Chippa's information, this

motion can only outline the possible bases for suppression for the Court to examine and consider.[1]

I. The Foreign Intelligence Surveillance Act

A. Legal background

FISA was enacted in 1978 in the wake of domestic surveillance abuses by federal law enforcement agencies as cataloged in Congressional Committee and Presidential Commission Reports.[2] The statute was designed to provide a codified framework for foreign intelligence gathering within the confines of the United States in response to civil liberties concerns and the gap in the law noted by the Supreme Court in *United States v. United States District Court* (Keith, J.), 407 U.S. 297, 308-09 (1972)(hereinafter "*Keith*").

Through FISA, Congress attempted to limit the ability of the Executive Branch to engage in abusive or politically motivated surveillance. FISA constituted

---

[1] Mr. Chhipa notes the adverse rulings in the Fourth Circuit cases, *United States v. Kokayi*, No. 19-4510, 2021 WL 3733010, at *6 (4th Cir. Aug. 24, 2021) and *United States v. Dhirane*, 896 F.3d 295, 301 (4th Cir. 2018) on some of these issues. Mr. Chhipa recognizes that the legal precedents are binding on this Court. Nevertheless, he asserts these arguments on a different set of facts, as well as for preservation purposes, because these cases did not address the FAA, and because the Foreign Intelligence Surveillance Court (FISC) has since revealed more recent abuses of process since one or both of these opinions.

[2] *See, e.g.*, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. Rep. No. 94-755, 94th Cong., 2d Sess. (1976); Commission on CIA Activities Within the United States, Report to the President (1975) (commonly referred to as the "Rockefeller Commission Report"). *See also United States v. Belfield*, 692 F.2d 141, 145 (D.C. Cir. 1982) ("[r]esponding to post-Watergate concerns about the Executive's use of warrantless electronic surveillance, Congress, with the support of the Justice Department, acted in 1978 to establish a regularized procedure for use in the foreign intelligence and counterintelligence field").

Congress' attempt to balance the "competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the Nation, and the requirements of the Fourth Amendment." H.R. Rep. No. 95-1283, at 15; *see also In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (FISA "was enacted in 1978 to establish procedures for the use of electronic surveillance in gathering foreign intelligence information. . . . The Act was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties") (quotation omitted).

Significant differences exist between the standards for a FISA warrant and warrants issued under the Fourth Amendment or Title III of the U.S. Criminal Code. The "probable cause" required under FISA is merely that the "target" qualifies as an "agent of a foreign power," 50 U.S.C. § 1801(b), who uses, owns, possesses the electronic device subject to electronic surveillance or such devices in the premises to be searched, *see* 50 U.S.C. §§ 1805(a)(3) & 1824(a)(3), and not that a crime has been, or is being, committed.

In that context, FISA establishes procedures for surveillance of foreign intelligence targets, whereby a federal officer acting through the Attorney General may obtain judicial approval for conducting electronic surveillance for foreign intelligence purposes. The FISA statute created a special FISA Court – the Foreign Intelligence Surveillance Court (hereinafter "FISC") – to which the Attorney General must apply for orders approving electronic surveillance of a foreign power,

or an agent of a foreign power, to obtain foreign intelligence information. See 50 U.S.C. §§1802(b), 1803 & 1804.[3]

In considering an application for electronic surveillance under FISA, the FISA court determines whether the application meets the following criteria sufficient to permit the Court to make the requisite findings under §1805(a):

(i) that the application was made by a federal officer and approved by the Attorney General;

(ii) that there exists probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and . . . each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or agent of a foreign power[;]"

(iii) that the proposed minimization procedures meet the definition of minimization procedures under §1801(h); and

(iv) that the application contains all required statements and certifications.

Also, in accordance with §1805(a)(4), if a target is a "United States person,"[4] the FISC must determine whether the "certifications" under §1804(a)(6)(E) are "not clearly erroneous" – namely that the information sought is "the type of foreign intelligence information designated," and the information "cannot reasonably be obtained by normal investigative techniques." In addition, §1805(a)(2)(A) provides

[3] The FISC consists of eleven judges (previously seven prior to amendments adopted as part of the The USA PATRIOT Act) who individually hear government applications. *See* 50 U.S.C. § 1803.

[4] As a naturalized U.S. citizen, Mr. Chhipa qualifies as a "United States person" under §1801(i).

"that no United States person may be considered a foreign power . . . solely upon the basis of activities protected by the first amendment . . ."

FISA authorizes any "aggrieved person" to move to suppress evidence obtained or derived from an electronic surveillance because "the information was unlawfully acquired" or "the surveillance was not made in conformity with an order of authorization or approval." §§ 1806(e)(1) & (2); 1825(f). FISA defines an "aggrieved person" as "a person who is the target of electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." §1801(k).

FISA also permits evidence generated in intelligence investigations to be used in criminal prosecutions. §§ 1806(b) & 1825(c). However, if a significant purpose of the surveillance is not to obtain foreign intelligence information but rather for a criminal investigation, obtaining that evidence without complying with the Fourth Amendment violates the Constitution. *See* § 1804(a)(6)(B).

B. Challenges to the admissibility of FISA-generated evidence

i. Grounds upon which the FISA applications may fail to establish the requisite probable cause.

Because Mr. Chhipa has been notified that his communications and/or property have been the subject of FISA surveillance and searches, he is an "aggrieved person" under § 1806(k). While aggrieved criminal defendants can move to suppress FISA-generated evidence, §1806(f) provides that if the Attorney General files an affidavit that "disclosure or an adversary hearing would harm the national security of the United States," the court deciding the motion must consider the

application and order for electronic surveillance *in camera* to determine whether the surveillance was conducted lawfully. Accordingly, FISA "requires the judge to review the FISA materials *ex parte in camera* in *every* case" to "decide whether any of those materials must be disclosed to defense counsel." *United States v. Daoud*, 755 F.3d 479, 482 (7th Cir. 2014).

The statute also adds that "[i]n making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Alternatively, § 1806(g) provides that "[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure."

Defense counsel in this case has not been provided with the FISA applications that resulted in the surveillance and searches at issue. The lack of access to the underlying FISA applications presents a significant impediment to asserting a challenge to FISA surveillance with particularity. As the Fourth Circuit has recognized in an analogous context, the burden of being specific with respect to the basis for suppression must be relaxed when the information supporting the motion is held uniquely by the government. *See United States v. Moussaoui*, 382 F.3d 453, 472 (4th Cir. 2004) ("Because Moussaoui has not had—and will not receive—direct access to any of the witnesses, he cannot be required to show

materiality with the degree of specificity that applies in the ordinary case.")(citing *United States v. Valenzuela-Bernal*, 458 U.S. 858, 870-71, 873 (1982)).

a) The elements of probable cause under FISA

Before authorizing FISA surveillance, the FISA Court must find, *inter alia*, probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power." §1805(a)(2)(A). The Supreme Court has reiterated the long-standing rule that criminal probable cause requires "a reasonable ground for belief of guilt," and that "the belief of guilt must be particularized with respect to the person to be searched or seized." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Under FISA, though, unlike a traditional warrant, the probable cause standard is directed not at the target's alleged commission of a crime, but at the target's alleged status as "a foreign power or an agent of a foreign power. This Court must engage in the same analysis for each application at issue here. §§1805(a)(2)(A) & 1801(b)(2)(C) & (E).

b) The "Agent of a Foreign Power" requirement

Here, absent an opportunity to review the applications for any of the surveillance at issue, defense counsel cannot specify whether the allegations that the defendants were an "agent of a foreign power" were sufficient to satisfy FISA. Among FISA's definitions of "agent of a foreign power," §1801(b)(2)(C) provides that the term includes: "any person . . . who *knowingly* engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." (emphasis added).

If that provision was, in fact, the basis for the FISA applications, the statute requires the presentation of evidence establishing probable cause that the defendant or the relevant third-party target knowingly engaged in some type of international terrorism, and that the defendant *knew* that his activities were assisting "international terrorism."

c) The nature and origins of the information in the FISA applications

Again, unlike the case with traditional warrants, non-disclosure of the FISA applications denies the defense the ability to contest the accuracy or reliability of the underlying information used to satisfy FISA's version of probable cause. As a result, absent such disclosure the defendant can request only that the Court review the FISA applications cognizant of certain factors and principles.

1) The limits of "raw intelligence"

Foreign intelligence information is often presented in "raw" form, and not vetted in the manner typical of information law enforcement agents supply in ordinary warrant applications, *i.e.*, that the information emanated from a source that was reliable and/or had a verifiable track record, or was independently corroborated. Raw intelligence is often not attributed to any specific source, and its genesis can be multiple-level hearsay, rumor, surmise, and rank speculation. Also, the motivation driving sources of raw intelligence to impart information is usually not nearly as transparent as in conventional criminal justice circumstances. As a result, the dangers of deception and disinformation are significantly enhanced.

In this case, we know that some of the material involving Mr. Chhipa was derived from foreign intelligence. *See infra* footnote 26 (citing search warrants 20-sw-1559; 23-sw-236)(stating "a foreign government provided the FBI with information…"; and "information was provided by a foreign government…"). Those limitations on the accuracy and reliability of raw intelligence are aggravated when the potential location – Syria, a nation afflicted by conflict, and to which the U.S. government has limited access – and context – often military and susceptible to the "fog of war" – reduce the possibility of meaningful corroboration or verification. *Latif v. Obama*, 666 F.3d 746, 771 (D.C. Cir. 2011) (Tatel, J., dissenting) (discussing the problems inherent in the "presumption of regularity" accorded government intelligence reports in the context of habeas corpus petitions filed by Guantanamo Bay detainees).

2) Illegitimate and/or illegal sources of information

There is also the danger that the information in FISA applications, whether or not attributed to a particular source, was generated by illegal means such as warrantless wiretapping or constitutionally infirm FISA Amendments that have barely been challenged in criminal cases and not in the Fourth Circuit. *See infra* Part II, FISA Amendments Act. In that context, the government should be compelled to disclose whether information in the FISA applications were derived from these means. *Cf. Gelbard v. United States*, 408 U.S. 41 (1972) (in prosecution for contempt for refusal to testify, grand jury witness entitled to invoke as a defense

statutory bar against use of evidence obtained via illegal wiretap as basis for questions in grand jury).

The government should not have any legitimate interest in obscuring the authority pursuant to which it conducted FISA surveillance herein. Refusal by the government to disclose would deny the defendants a fair trial by depriving him of any meaningful opportunity to contest the acquisition and admissibility of evidence. Accordingly, an examination of the nature and provenance of the information in the FISA application for Mr. Chhipa is critical, and this Court should compel the government to disclose whether any such information was the product of warrantless electronic surveillance, including but not limited the following examples of warrantless surveillance.

In drafting and submitting the FISA Applications here, the government may have used, and should be required to disclose whether it did use, any of the defendant's communications intercepted pursuant to the Terrorist Surveillance Program (hereinafter "TSP"), a warrantless wiretapping program instituted in 2001. *But cf. United States v. Abu Ali*, 528 F.3d 210, 257 (4th Cir. 2008) (affirming district court's conclusion that disclosure of TSP was not warranted based on *ex parte* review of government justification). These interceptions may have either directly been used in the FISA Application, or indirectly contributed to the justifications presented in the FISA Application.

Relatedly, the FISA Application may also have directly or indirectly relied on Section 702 material that was undoubtedly collected in this case. The legal

infirmities of Section 702, some of which have been recognized by the FISC itself, are detailed *infra* Part II, FISA Amendments Act. Reliance on material generated from Section 702, directly or indirectly, in a FISA application implicates serious concerns of process and constitutional transgressions.

The government employs other powerful and controversial surveillance tools under Executive Order 12333.[5] Unlike Section 702 surveillance, E.O. 12333 surveillance typically occurs outside the United States. Using this authority, the NSA intercepts the contents and records of phone calls, video chats, emails, internet activity, and text messages—often in bulk, and all without a warrant. *See* PSLOB 2023 Report at 173 ("[I]n some circumstances, the government may be able to use E.O. 12333 or, for certain metadata, National Security Letters, to obtain information similar to that collected under Section 702.… it is worth emphasizing that Section 702 provides stronger privacy safeguards than either E.O.12333 or National Security Letters.")(citation omitted). Because Americans routinely communicate with people and organizations located overseas, as Mr. Chhipa is alleged to have, their communications are swept up in large quantities.[6]

In this case it is clear that the FBI received information on Chhipa from obscured sources. *See infra* Part II. For example, the FBI stated that it re-initiated a full investigation into Mr. Chhipa after reviewing some questionable facebook

---

[5] E.O. 12333, as amended, available at https://bit.ly/2GNTqqq.

[6] *See, e.g.*, Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times, Aug. 13, 2014, https://nyti.ms/2L9cROa; John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014, http://wapo.st/1wPuzv2.

posts from a carl johnson facebook account on March 15, 2019. *See* Def.'s Ex. 1 at 5. The government requested and received records for that facebook account on March 19, 2019. Those facebook records returned one particular email address. *See* Def.'s Ex. 5. Yet just a day later the government issued a grand jury subpoena for a separate email address with no indication as to how the government would have known about that email address at that point. *See* Def.'s Ex. 4.

Additionally, a March 2019 FBI report less than two weeks later contains a list of selectors or "facilities" (email addresses and phone numbers) that pre-date the returns from the service providers containing those identifiers. *Compare* Def.'s Ex. 2 at 9-10 *with* Def.'s Ex. 3 at 4-5. Another FBI report, (Def.'s Ex. 2 at 4) is heavily redacted and provides limited information on the methods of collection that "revealed" these accounts, but does include "surveillance" as one of the "tools used to date" as of March 2019.

Thus, there are multiple strong indications that that the government was surveilling Mr. Chhipa under some other type of intelligence program prior to the search warrants issued in 2019 and using that information to form the basis for probable cause in a search warrant ordered by a court. It is unknown what information was used for probable cause in the FISA applications against Mr. Chhipa. Obscuring the source of the information contained in the search warrants and FISA warrants limits Mr. Chhipa's ability to challenge the violations and to move for suppression of the resulting derivative material.

ii. The application may violate FISA's prohibition on basing probable cause solely on a "United States Person's" protected First Amendment activity.

FISA prohibits finding probable cause for a "United States person" based solely upon First Amendment activities. §1805(a)(2)(A). Accordingly, if the target participated in First Amendment activities such as expressing support, urging others to express support, gathering information, distributing information, raising money for political causes, or donating money for political causes, these activities cannot serve as a basis for probable cause for a FISA warrant. The statute reaches only material support coordinated with or under the direction of a designated foreign terrorist organization. *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 31-32 (2010) ("Independent advocacy that might be viewed as promoting the group's legitimacy is not covered."). In fact here, the Indictment does not allege any material support by Mr. Chhipa to ISIS until 2019. Yet the investigation of him began in 2008. Def.'s Exs. 1, 2, and 3. It also indicates that the investigation against Mr. Chhipa was reopened in part because of posts of quotations "from radical clerics espousing an extremist ideology." Def.'s Ex. 2 at 3. That raises the obvious question of whether there was any basis, other than protected First Amendment activity, for commencing FISA surveillance on Mr. Chhipa. Should the answer be in the negative, the FISA surveillance would be invalid under §1805(a)(2)(A).

iii. The FISA applications may contain intentional or reckless falsehoods or omissions in contravention of Franks v. Delaware, 438 U.S. 154 (1978).

The Supreme Court's landmark decision in *Franks v. Delaware*, 438 U.S. 154 (1978), established the circumstances under which the target of a search may obtain an evidentiary hearing concerning the veracity of the information set forth in a search warrant affidavit. As the Court in *Franks* instructed, "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statements necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Id*. at 156-57.

The Franks opinion also sets a similar standard for suppression following the evidentiary hearing:

> [I]n the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

Id., at 156; *see United States v. Blackmon*, 273 F.3d 1204, 1208-10 (9th Cir. 2001) (applying *Franks* to Title III wiretap application); *United States v. Duggan*, 743 F.2d 59, 77 n.6 (2d Cir. 1984) (suggesting that *Franks* applies to FISA applications under Fourth and Fifth Amendments).

The *Franks* principles apply to omissions as well as to false statements. *See, e.g., United States v. Carpenter*, 360 F.3d 591, 596-97 (6th Cir. 2004); *United States v. Atkin*, 107 F.3d 1213, 1216-17 (6th Cir. 1997). Omissions will trigger suppression under *Franks* if they are deliberate or reckless, and if the search warrant affidavit, with omitted material added, would not have established probable cause.

As noted above, without the opportunity to review the applications, the defendants cannot point to or identify any specific false statements or material omissions in those applications. *See Daoud*, 755 F.3d at 493 (Rovner, J., concurring) (explaining difficulty of reconciling *Franks* with denying access to FISA warrant applications, and concluding that "[w]ithout access to the FISA application, it is doubtful that a defendant could ever make a preliminary showing sufficient to trigger a *Franks* hearing."). Although that lack of access prevents defense counsel from making the showing that *Franks* ordinarily requires, counsel notes that the possibility that the government has submitted FISA applications with intentionally or recklessly false statements or material omissions is hardly speculative.

For instance, in 2002, in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISC), rev'd on other grounds sub nom., *In re Sealed Case*, 310 F.3d 717 (FISCR 2002),[7] the FISC reported that beginning in March 2000, the Department of Justice (hereinafter "DOJ") had come "forward to confess error in some 75 FISA applications related to

[7] "FISCR" refers to the Foreign Intelligence Court of Review, which is the appellate court for the FISC, and is comprised of three federal circuit judges. The FISCR's 2002 decision in *In re Sealed Case* marked its first case since enactment of FISA in 1978.

major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts," including:

- the government's failure to apprise the FISC of the existence and/or status of criminal investigations of the target(s) of FISA surveillance; and
- improper contacts between criminal and intelligence investigators with respect to certain FISA applications. *Id*.

According to the FISC, "[i]n March of 2001, the government reported similar misstatements in another series of FISA applications . . ." *Id*. at 621. These problems were not resolved by those revelations. A report issued March 8, 2006 by the DOJ Inspector General stated that the FBI found apparent violations of its own wiretapping and other intelligence-gathering procedures more than 100 times in the preceding two years, and problems appear to have grown more frequent in some crucial respects. *See Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act*, March 8, 2006.

The report characterized some violations as "significant," including wiretaps that were much broader in scope than authorized by a court ("over-collection"), and others that continued for weeks and months longer than authorized ("overruns"). *Id*. at 24-25. FISA-related overcollection violations constituted 69% of the reported violations in 2005, an increase from 48% in 2004. *See DOJ IG Report*, at 29. The total percentage of FISA-related violations rose from 71% to 78% from 2004 to 2005, *id*. at 29, although the amount of time "over-collection" and "overruns" were permitted to continue before the violations were recognized or corrected decreased from 2004 to 2005. *Id*. at 25.

These transgressions are not isolated to the early 2000s. Just recently, in 2020, the DOJ declared invalid two of the four surveillance warrants against former Trump campaign associate Carter Page. These were FISA applications that had been reviewed and approved by the FISC. Yet a subsequent scathing 400-plus page OIG report examined the DOJ's four FISA applications and the FBI's Crossfire Hurricane Investigation and found significant problems with material that had been submitted to the FISA Court. *See* DOJ OIG, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (Dec. 2019 (revised)).[8] Thus, after an internal DOJ review, the same court that had approved the FISA applications was subsequently noticed of "material misstatements and omissions in the [FISA] applications filed by the government." *Id.*

The corresponding FISC opinion offered a heavy rebuke of the FBI's FISA practices. It wrote:

> This order responds to reports that personnel of the Federal Bureau of Investigation (FBI) provided false information to the National Security Division (NSD) of the Department of Justice, and withheld material information from NSD which was detrimental to the FBI's case, in connection with four applications to the Foreign Intelligence Surveillance Court (FISC) for authority to conduct electronic surveillance of a U.S. citizen named Carter W. Page. When FBI personnel mislead NSD in the ways described above, they equally mislead the FISC.

In re Accuracy Concerns Regarding FBI Matters Submitted to FISC, 411 F. Supp. 3d 333, 334–35 (Foreign Intel. Surv. Ct. 2019)(hereinafter *Accuracy Concerns Regarding FBI Matters Submitted to FISC*).

[8] https://www.justice.gov/storage/120919-examination.pdf

The FISC also detailed how FBI personnel made frequent representations in FISA warrant applications that were "unsupported or contradicted by information in their possession," and "withheld information detrimental to their case." *Id.* at 337. This conduct, the FISC explained, was "antithetical to the heightened duty of candor" necessary in the *ex parte* context. *Id.* More broadly, the FISC stated that this issue "calls into question whether information contained in other FBI applications is reliable." *Id.* (emphasis added).

One must wonder whether this FISA surveillance would have simply been business as usual had the nature of the investigation not been so controversial. That Mr. Chhipa's case does not possess the elevated political profile of a prominent campaign associate should not preclude his situation from meaningful, adversarial review. In this case, an indication is already raised that there may be a *Franks* issue given that Def.'s Exhibit 2 (at 9-10) allegedly contains identifiers for Mr. Chhipa in March 2019 that would not have been known to the government based on the information it had at that time. *See* Def.'s Exhibit 3 at 5. But even without this indication, a *Franks* hearing, and disclosure of the underlying FISA materials, are necessary to permit the defendants the opportunity to prove that the affiants before the FISC intentionally or recklessly made materially false statements and omitted material information from the FISA applications as it has done before.

iv. The collection of foreign intelligence information may not be a significant purpose of the FISA surveillance.

The FBI had been investigating Mr. Chhipa since 2009. This indicates that Mr. Chhipa was a long-time criminal target, including at one point for a fraud

investigation related to student loans. To determine whether the collection of foreign intelligence information was either a "significant" or the "primary" purpose of the FISA surveillance, or whether it was a criminal investigation that motivated the FISA surveillance, the Court should order the government to disclose the FISA applications and related materials to the defense to allow the defense to provide input to the Court regarding these crucial determinations.[9]

If a significant purpose of the FISA surveillance was not pursuant to foreign intelligence gathering, but in fact criminal in nature, all of the evidence derived from the FISA surveillance of the defendant should be suppressed because the applications failed to adhere to FISA's requirements, and the government should have sought appropriate authority under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 99 2510-2520 (1982), rather than under

---

[9] Effective October 26, 2001, Congress amended §1804(a)(6)(B) through the USA PATRIOT Act to require government certification only that "a significant purpose" – rather than "the purpose" – of the surveillance is to obtain foreign intelligence information. In May, 2002, the FISCR, a federal court empowered to review the denial of a FISA application by the FISA Court, issued its first ever opinion in its 24-year history, in which, in dicta, it endorsed the "significant" purpose standard's constitutionality. *See In re Sealed Case*, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002). *See also United States v. Abu Jihaad*, 630 F.3d 102, 120 (2d Cir. 2010), and cases cited therein, *but see Mayfield v. United States*, 504 F.Supp.2d 1023 (D.Or.2007)(holding FISA violated the Fourth Amendment) *vacated on other grounds in* 599 F.3d 964 (9th Cir.2010) (holding that plaintiff lacked standing to seek declaratory relief against the United States and declining to address the Fourth Amendment issue). While Mr. Chhipa recognizes that the only Circuit decisions on this point are adverse, he nevertheless preserves a challenge to the constitutionality of this amendment, arguing that the "significant purpose" standard violates his Fourth Amendment rights because "FISA now permits the Executive Branch to conduct surveillance and searches of American citizens without satisfying the probable cause requirements of the Fourth Amendment." *Mayfield*, 504 F.Supp.2nd at 1039.

FISA. For example, the Privacy and Civil Liberties Oversight Board (PCLOB)[10] recently found that, in the Section 702 context

> [A]fter reviewing individual tasking sheets, the Board has identified instances in which analysts' written foreign intelligence justifications lack sufficient detail. Although the tasking sheets reviewed by the Board included documentation to demonstrate that targets were reasonably believed to be non-U.S. persons located outside the United States, the documentation of the foreign intelligence purpose for the targeting was not similarly thorough or sufficiently detailed. The tasking sheets stated the foreign intelligence purpose but did not describe or document why the particular target was expected to possess or communicate such information. For example, tasking sheets stated that the target was a member of a particular terrorist group without documenting the basis for this conclusion.

PCLOB 2023 Report at 173.

v. The FISA applications may not have included the required certifications.

The Court should review the FISA applications to determine whether they contain all certifications required by §1804(a)(6). As the Ninth Circuit has declared in the Title III context, "[t]he procedural steps provided in the Act require 'strict adherence,'" and "utmost scrutiny must be exercised to determine whether wiretap orders conform to [the statutory requirement]." *Blackmon*, 273 F.3d at 1207, quoting *United States v. Kalustian*, 529 F.2d 585, 588-9 (9th Cir. 1975).

In addition, the Court should examine two certifications with particular care – (i) that the information sought is "the type of foreign intelligence information

---

[10] The PCLOB is an independent agency within the executive branch, authorized by statute, inter alia, to "analyze and review actions the executive branch takes" and "ensure that liberty concerns are appropriately considered" in the government's development and implementation of anti-terrorism programs. *See* 42 U.S.C. § 2000ee(c). The PCLOB is composed of five members, appointed by the President and confirmed by the Senate. *Id*. § 2000ee(h).

designated," and (ii) that the information "cannot reasonably be obtained by normal investigative techniques." *See* §1804(a)(6)(E). Particularly if the target of the wiretap is a "United States person" (such as Mr. Chhipa), these two certifications must be measured by the "clearly erroneous" standard. *See* §1805(a)(4).

As the Ninth Circuit has observed in relation to the similar provision in Title III, 18 U.S.C. § 2518(1)(e), "the necessity requirement 'exists in order to limit the use of wiretaps, which are highly intrusive.'" *Blackmon*, 273 F.3d at 1207, quoting *United States v. Bennett*, 219 F.3d 1117, 1121 (9th Cir. 2000) (internal quotation omitted). The necessity requirement "ensure[s] that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the [information sought]." *Id*. In this case, among other surveillance, the government intercepted and collected Mr. Chhipa's personal phone calls from in 2019 to 2022. There appears little reason as to why the government could not have properly sought a Title III warrant for this "highly intrusive" wiretap. *Id.*

The Court should also carefully examine the dates, in sequence, of all FISA orders in this case to determine whether there were any lapses of time during which wiretapping continued, or whether any FISA surveillance continued after Mr. Chhipa became the target of a criminal investigation. The statutory scheme contemplates that when a FISA order expires and the government wishes to continue the wiretap, the expiring order must be replaced by an extension order, which, in turn, may be obtained only on the basis of a proper FISA application. *See* §1805(d)(1) & (2).

FISA surveillance that continues past the expiration date of the FISA order that originally authorized it is just as unauthorized as a wiretap that is initiated without any FISA order at all. Should the Court order the government to disclose the FISA orders in this case to defense counsel, the defense will be able to assist the Court in matching up all of the FISA orders by date – an arduous, albeit necessary, task.

vi. The FISA applications, and the FISA surveillance, may not have contained or implemented the requisite minimization procedures.

In order to obtain a valid FISA order, the government must include in its application a "statement of the proposed minimization procedures." §1804(a)(4). The purpose of these minimization procedures is to (i) ensure that surveillance is reasonably designed to minimize the acquisition and retention of private information regarding people who are being wiretapped; (ii) prevent dissemination of non-foreign intelligence information; and (iii) prevent the disclosure, use, or retention of information for longer than seventy-two hours unless a longer period is approved by Court order. §1801(h).

FISA surveillance involves particularly intrusive electronic surveillance. Indeed, it typically occurs on a continuance 24-hour basis, as the Title III principle of "pertinence" is not applicable. Instead, all conversations are captured, with minimization occurring later. Accordingly, minimization in the FISA context is critically important.

One court has reasoned that in FISA the privacy rights of individuals are ensured not through mandatory disclosure of FISA applications, but

> through its provisions for in-depth oversight of FISA surveillance *by all three branches of government* and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance.

United States v. Belfield, 692 F.2d 141, 148 & n. 34 (D.C. Cir. 1982) (footnote omitted), quoting Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Job*, 12 RUTGERS L.J. 405, 408 (1981) (emphasis added). Here, the government has provided an incredibly large amount of intercepted material going back at least to 2019. It is possible that the FISA application did not contain adequate minimization procedures or, if it did, that those procedures were not followed.

C. FISA mandates suppression when a court concludes that surveillance was unlawful.

Not only is Mr. Chhipa entitled to suppression under the Fourth Amendment, but FISA itself provides a mandatory statutory remedy. If the Court "determines that the surveillance was not lawfully authorized or conducted, it shall . . . suppress the evidence which was unlawfully obtained or derived" from such surveillance. 50 U.S.C. § 1806(g) (emphasis added). "This ground for suppression plainly includes constitutional challenges to FISA itself." David S. Kris & J. Douglas Wilson, 2 *National Security Investigations & Prosecutions* § 32:3 (2d ed. 2012). Thus, if the Court finds that the government's surveillance of Mr. Chhipa's communications was unlawful in this case, he is entitled to suppression under Section 1806(g).

II. FISA Amendments Act

A. Legal background

Section 702 of FISA, 50 .S.C. § 1881a, was enacted in 2008 as part of the FISA Amendments Act (the FAA). However, for seven years prior to the passage of the FAA, NSA had been conducting (at least) the very same electronic surveillance and interception ultimately authorized by the FAA. For example, "in 2001, the NSA began acquiring Internet-based communications of overseas targets without the use of a traditional law enforcement warrant or an electronic surveillance order under Title I of FISA." Edward C. Liu, Andrew Nolan, Richard M. Thompson II, *Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments*, Congressional Research Service at 10 (April 1, 2014) (hereinafter "CRS Report: Overview")(citing, December 20, 2013, *Unclassified Declaration of Frances J. Flesch*, National Security Agency, in *Schubert v. Obama*, 07 Civ. 693 (JSW) (N.D.Cal.)).[11]

Initially, such surveillance and interception was performed through the TSP and without any legislative or court authorization. *See* James Risen & Eric Lichtblau, *Bush Let U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005).[12] After the TSP's existence was disclosed in December 2005 in the New York Times, legislation followed. "Utimately, new statutory authority for this type of acquisition was provided, at first, temporarily under the Protect America Act

[11] https://sgp.fas.org/crs/intel/R43459.pdf
[12] https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

('PAA') of 2007 [P.L. 110-55], and on a longer term basis by the FISA Amendments Act ('FAA') [P.L. 261]." CRS Report: Overview, at 10 (footnotes omitted).

Section 702 radically increased the Government's ability to search and seize the private electronic communications of U.S. citizens and all those protected by the Fourth Amendment. While FISA itself already represented novel authorizations for electronic eavesdropping abandoning substantive and procedural requirements present in Title III, Section 702 further extended the distance from traditional Fourth Amendment warrant requirements. The FAA allows the Government to surveil and collect information on any "non-U.S. person" – which includes "any group, entity, association, corporation, or foreign power" (50 U.S.C. § 1801(m)) – that is located overseas so long as a "significant" purpose of that interception is related to foreign intelligence, which is broadly defined. *See* 50 U.S.C. § 1801(e).

B. The manner in which the FAA is implemented

While the statute is complex, its purpose and effect are straightforward: to permit the broad surveillance of digital communications entering and leaving the United States, with limited court involvement. Section 702 surveillance does not require a probable cause determination or for the Government to submit a FISA application specifying the nature and location of each of the particular facilities or places at which the electronic surveillance will occur. *See United States v. Hasbajrami*, 945 F.3d 641, 651 (2d Cir. 2019). Instead, the FISC approves the government's Section 702 procedures in advance through annual applications for certifications, and the government does not have to return to the FISC to seek approval before it undertakes surveillance of any specific individual. *See id.*

The certifications the government submits to the FISC in advance for approval require the Attorney General (AG) and Director of National Intelligence (DNI) to develop "targeting," "minimization," and "querying" procedures. *United States v. Muhtorov*, 20 F.4th 558, 587 (10th Cir. 2021) (citing § 1881a(d)(1), (e)(1), (f)(1)). "These procedures govern how the program functions at each agency tasked with Section 702 surveillance—the NSA, the FBI, and the Central Intelligence Agency (CIA)." *Id.* (cleaned up). The FISC's role consists principally of reviewing these general rules that the government proposes to use in carrying out the surveillance. *Id.* § 1881a(j).

The government needs not ever inform the FISC of whom it intends to target or on what factual basis. And, critically, the government need not even seek a warrant when its agents decide to peruse the communications of Americans swept up in this surveillance. Instead, agents have wide latitude to sift through the communications pulled in under Section 702—including in the course of investigating Americans. While the PCLOB described Section 702 in its most recent report as highly valuable to national security, in the same breath it states that Section 702 "creates serious privacy and civil liberties risks." *See* Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702* at 7 (Sept. 28, 2023)(hereinafter "PCLOB 2023 Report").[13] It found that "the risk of overbroad government collection of communications under Section

[13] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

702 and subsequent government use of that information is very real and can cause harm, at varying degrees." *Id.* at 9.

i. Targeting

"Targeting generally refers to the decision to surveil an individual or his or her channels of electronic communications, such as an e-mail address." *Hasbajrami*, 945 F.3d at 652. The government need not demonstrate to any court that the people it seeks to surveil are agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Instead, Section 702 permits the government to target *any* foreigner located outside the United States to obtain "foreign intelligence information"—a term broadly defined to encompass nearly any information bearing on the foreign affairs of the United States. *See* 50 U.S.C. § 1881a(a).

According to 50 U.S.C. §§ 1881a(b)(1), (3), the government may not "intentionally target" a person located in the United States or a "United States person" outside the United States. *Id.* Moreover, the government may not target a non-United States person "if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a(b)(2).

After approval by the FISC, "an agency can begin surveilling individuals it seeks to target. The NSA initiates all Section 702 targeting, and thus makes all initial decisions pursuant to its targeting procedures….[T]he CIA and the FBI can 'nominate' targets to the NSA for Section 702 targeting but the NSA is required to make the determination whether to initiate targeting." *Id.* at 652-53 (cleaned up).

"[T]he government may use Section 702 information in criminal prosecutions including prosecutions unrelated to the purpose of the original targeting." PCLOB 2023 Report at 180 (citing 50 U.S.C. § 1881e(a)).

ii. Collection and Minimization

Section 702 collection is incredibly robust. The government "targets" more than 200,000 people annually overseas and, in so doing, sweeps in billions of electronic communications, including Americans' communications. *See* Office of the Director of National Intelligence, *2023 Statistical Transparency Report* at 18 ("ODNI 2023 Statistical Transparency Report"). [14] The government reported that, in 2022, it monitored the communications of 246,073 targets under a single mass surveillance order. *Id.* In 2011, when it monitored approximately 35,000 unique selectors,[15] the government still collected more than 250 million communications.[16] Thus, today, with 246,073 targets (which represents a 276% increase since CY2013, *see* PCLOB 2023 Report at 172) the government likely collects over a billion communications under Section 702 each year. *See also* PCLOB 2023 Report at 61 ("As of 2021, NSA acquired approximately 85.3 million Internet transactions a year from upstream collection, which represents a small portion of NSA's Section 702

---

[14], https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf

[15] "Selectors may be communications facilities that are assessed to be used by the target, such as the target's email address or telephone number." *See* PCLOB 2023 Report at 3; Glenn Greenwald, *No Place to Hide* 111 (2014), https://perma.cc/6VU2-5RNH (NSA documents showing that 35,000 "unique selectors" were surveilled under PRISM in 2011).

[16] *See* Redacted, 2011 WL 10945618, at *9 (Foreign Intel. Surv. Ct. Oct. 3, 2011)

collection."). Section 702 reaches every form of modern electronic communication: telephone calls, emails, video calls, texts, and online chats, among others.[17]

Although the government targets a significant number of persons under Section 702, the number of "targets" does not reflect the true scope of the surveillance. "While Section 702 relies upon individual targeting decisions by analysts, the government is able to acquire and store substantial amounts of data—including incidentally collected U.S. person information—that goes beyond what the government could collect under other authorities such as Title I of FISA, because the standards for targeting under Section 702 are by design less rigorous than those governing surveillance targeting persons within the United States." PCLOB 2023 Report at 172. The Washington Post's review of a "large cache of intercepted conversations" revealed that the vast majority of people subject to surveillance "were not the intended surveillance targets but were caught in a net the agency had cast for somebody else."[18] The 2014 material reviewed by the Post consisted of 160,000 intercepted email and instant message conversations, 7,900 documents—including "medical records sent from one family member to another, resumes from job hunters and academic transcripts of schoolchildren"—and more than 5,000 private photos. *Id.* From what we know, "[t]he NSA operates two separate types of collection programs which collect different types of information. These two

---

[17] *NSA Slides Explain the PRISM Data-Collection Program*, Wash. Post, Jun. 6, 2013, http://wapo.st/J2gkLY

[18] Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, Jul. 5, 2014, http://wapo.st/1MVootx.

programs have come to be labelled PRISM collection and upstream collection." *Hasbajrami*, 945 F.3d at 652.

a) PRISM collection

The PRISM program resembles a traditional wiretap. "The FBI (on behalf of the NSA) sends 'selectors' (for instance, an e-mail address) to internet service providers ("ISPs"), based in the United States." *Id.* That ISP then sends the NSA all emails sent to or from that selector. *See id.* This collection occurs roughly in real time, and the materials are "monitored and analyzed at or near the time of their collection." *Id.*

b) Upstream collection

"Upstream collection is broader." *Id.* Rather than collect information from a particular ISP, upstream essentially collects data as it traverses the telecommunications system. *See id.* This allows the government to collect data that would otherwise be out of reach such as emails from a person using a foreign ISP. *See id.* By collecting data this way, upstream collection gathers more than a single email, it captures whole "multi-communication transactions," or "MCTs." *Id.* at 654 (citations omitted).

"If a single discrete communication within an MCT is to, from, or about a Section 702-tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire MCT" under upstream collection. The result is a greater

likelihood that upstream collection will result in the acquisition of wholly domestic communications and extraneous U.S. person information. The NSA is the only agency that receives upstream collection; the CIA and FBI are not provided with information obtained in this manner and do not store it in their databases." *Id.* (cleaned up).

c) Minimization

"In general terms, minimization describes the manner in which the government processes communications after they have been collected and seeks to provide safeguards against the misuse of Section 702 information." *Id.* at 655 (citation omitted). 50 U.S.C § 1881a(e)(2) requires that the NSA, FBI, and CIA seek yearly approval of their minimization procedures from the FISC, and "that each agency also adopt procedures that prohibit the disclosure of information about United States persons in a manner that identifies them, unless that identity is necessary to understand the intelligence information." *Id.* (citing 50 U.S.C. § 1881a(e)(1) (cross-referencing 50 U.S.C. §§ 1821(4) and 1801(h)).

Generally, this process involves an analyst's review of the data to determine if it should be retained or destroyed. "[I]nformation is 'minimized' by non-retention." *Id.* The NSA analysts are held to a "reasonable judgment" standard as to what is "relevant to the authorized purpose of the acquisition" when determining which material should be destroyed. *Id.*

> After an NSA analyst reviews an individual e-mail communication, he or she will decide if the information warrants retention in the NSA's databases and/or dissemination to other agencies. The analyst will determine if it is a domestic or foreign communication to, from, or about

> a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Communications fitting this description will thus be retained and processed; information not involving foreign intelligence information or evidence of a crime will be destroyed unless it meets one of several exceptions, such as when the communication contains information pertaining to a threat of serious harm to life or property.

Id. at 656 (cleaned up).

"Domestic communications" are considered communications that do not have at least one participant outside the United States. *Id.* These domestic communications are to"be promptly destroyed," except under certain conditions, including if a communication is "reasonably believed to contain significant foreign intelligence information." *Id.* (ciations omitted). In that case, "the domestic communication may be provided to the FBI (which in turn may disseminate information "in accordance with its minimization procedures"). *Id.* (citations omitted). "[I]nformation that is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed may be disseminated (including United States person identities) to appropriate Federal law enforcement agencies." *Id.* (citations omitted).

By ostensibly targeting foreign persons, the Government nonetheless searches and seizes the private communications of U.S. persons in contact with those foreign persons without complying with basic Fourth Amendment protections. The government describes the collections as either "incidental" (those U.S. persons whose communication is tied to the targeted foreign person) or "inadvertent" (a targeted person who mistakenly is actually a U.S. person). *See United States v. Hasbajrami*, 945 F.3d 641, 657 (2d Cir. 2019). "Since the enactment of Section 702,

the intelligence community has stated that it cannot provide metrics to identify the amount of incidentally collected U.S. person information under Section 702." PCLOB 2023 Report at 2.

Although the government euphemistically describes the collection of American communications as "inadvertent" and "incidental," these terms ignore what any reasonable individual with knowledge of the surveillance could foresee: the intrusions on U.S. persons are as inevitable and expected as the government's protestations to the contrary. This was acknowledged by the FISC in 2011 in [Redacted] 2011 WL 10945618, at *16:

> The government argues that an NSA analyst's post-acquisition discovery that a particular Internet transaction contains a wholly domestic communication should retroactively render NSA's acquisition of that transaction 'unintentional.'…. That argument is unavailing. NSA's collection devices are set to acquire transactions that contain a reference to the targeted selector. When the collection device acquires such a transaction, it is functioning precisely as it is intended, even when the transaction includes a wholly domestic communication. The language of the statute makes clear that it is the government's intention at the *time of acquisition* that matters, and the government conceded as much at the hearing in this matter…. Accordingly, the Court finds that NSA intentionally acquires Internet transactions that reference a tasked selector through its upstream collection with the knowledge that there are tens of thousands of wholly domestic communications contained within those transactions.

(emphasis in original; citations omitted).

It is unknown precisely how many Americans are swept up in the government's surveillance web. Despite repeated requests from members of Congress, the government has refused even to estimate the number of Americans' communications it collects under Section 702. By all accounts, however, the volume

is significant. The PCLOB wrote, "While the term [incidental] may make this collection sound insignificant, and we do not yet know the scope of incidental collection, it should not be understood as occurring infrequently or as an inconsequential part of the Section 702 program." PCLOB 2023 Report at 10.

In reality, the billions of communications intercepted under Section 702 are far too great in number for government analysts to review individually, let alone use. They are simply added to the government's massive databases of intercepted communications, to await later search, use, and analysis. *See* PCLOB 2023 Report at 139-155.

iii. Querying

The shear volume of 702-collected data renders it essentially meaningless without querying features. Reportedly, the NSA makes a copy of "nearly all cross-border text-based data," scans the content of each message using its chosen keywords, and then saves any communication that contains a match for further analysis. Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013.

"The NSA, CIA, and FBI each maintain separate databases containing Section 702 information on which the agencies rely for their own purposes." *Id.* at 657 (citations omitted). "While the government is restricted from targeting U.S. persons, agency procedures permit querying Section 702 collection using terms that identify one or more U.S. persons." PCLOB 2023 Report at 6. While other agencies

may only query data based on a reasonable belief that it will yield foreign intelligence information, the FBI is authorized to query the Section 702 database if it is "likely to retrieve evidence of a crime." *Id.*[19] The FBI is one of the four agencies that receives unminimized Section 702 data. *See id.* at 74.

"[T]hrough Section 702, the government amasses large databases of communications, including communications to or from United States persons in the United States. And the government may later query these databases, such as for a name or email address. After-the-fact queries are sometimes called 'backdoor searches.' " *United States v. Muhtorov*, 20 F.4th at 589 (citing *Hasbajrami*, 945 F.3d at 657). As a matter of course, "[t]he FBI also will query previously acquired information from a variety of sources, including Section 702 when it opens new national security investigations." *Hasbajrami*, 945 F.3d at 658 (citation omitted).

> The FBI's querying practices under Section 702 are especially important because the FBI conducts many more U.S.-person queries than the other agencies. In 2017, NCTC, the CIA, and NSA collectively used approximately 7500 terms associated with U.S. persons to query content information acquired under Section 702, while during the same year FBI personnel on a single system ran approximately 3.1 million queries against raw FISA-acquired information, including section 702-acquired information….The large number of U.S.-person queries run by the FBI makes its querying practices significant, despite its receiving only a small percentage of the total information acquired under Section 702.

[19] The FBI also employs "batch job queries," — queries through which FBI personnel search Section 702 information with hundreds or thousands of query terms at once—pursuant to the same justification. In June 2023, FBI began requiring attorney pre-query approval to conduct batch job queries of any size. *Id.* at 6, 8.

Redacted, 402 F. Supp. 3d 45, 75 (Foreign Intel. Surv. Ct. 2018), aff'd in part sub nom. *In re DNI/AG 702(h) Certifications 2018*, 941 F.3d 547 (Foreign Int. Surv. Ct. Rev. 2019) (cleaned up)(hereinafter "2018 FISC Opinion").

More recently, the ODNI 2023 Statistical Transparency Report shows a similar landscape. For statistics on the number of U.S. Person queries for the FBI the Report collectively shows (at 21):

Figure 9: **Number of U.S. Person Queries of Section 702 Combined Contents/Noncontents (FBI)**

Estimated number of U.S. Person queries of unminimized Section 702-aquired contents and noncontents	Duplicative Counting Method used in CY2021 Report	**De-duplicated Counting Method new for CY2022 Report (Unique Terms)**
December 2019–November 2020	1,324,057	**852,894**
December 2020–November 2021	3,394,053	**2,964,643**
December 2021–November 2022	204,090	**119,383**
% Reduction 2022 v. 2021	93.99%	95.97%
% Reduction 2022 v. 2020	84.59%	86.00%

The PCLOB wrote this past year that:

> The Board assesses that U.S. person queries present some of the most serious privacy and civil liberties harms. Except in the very limited circumstances covered by Section 702(f)(2) for certain FBI queries, government personnel are not required by Section 702 to make any showing of suspicion that the U.S. person is engaged in any form of wrongdoing prior to using a query term associated with that specific U.S. person. Nor does Section 702 require analysts or agents to seek approval from any judicial authority or other independent entity outside their agency. Americans' communications captured through surveillance can include discussions of political and religious views, personal financial information, mental and physical health information, and other sensitive data. Moreover, ordinary Americans may be in contact with Section 702 targets for business or personal reasons even if the Americans have no connection to, or reason to suspect, any wrongdoing by their foreign contacts and even when the government has no reason to believe the target has violated any U.S. law or engaged in any wrongdoing.

> Although all U.S. person queries by the Intelligence Community present privacy and civil liberties risks, FBI's querying procedures and practices pose the most significant threats to Americans' privacy. The Board recognizes and welcomes the fact that FBI has recently implemented several reforms designed to improve compliance, but these changes have not been sufficient to protect privacy and civil liberties. FBI's querying practices pose greater threats to privacy because FBI, as the United States' domestic law enforcement agency, has the ability and the mission to investigate and prosecute Americans for crimes. Further, FBI routinely searches Section 702 data at the pre-assessment and assessment stages of FBI investigations.

PCLOB 2023 Report at 10-11.[20]

The PCLOB recommended that Congress require FISC authorization of U.S.-person query terms. *Id.* at 12. The chair of the PCLOB wrote separately to say that this recommendation should be even stronger, and that it should require a showing of probable cause to the FISC. Specifically, the chair stated, that "this would ensure that such queries fully comply with the Fourth Amendment, and would be consistent with criminal law in other contexts.… [A] search through Section 702 communications data seeking information about a particular American constitutes a search under the Fourth Amendment, and current query standards are insufficient to meet constitutional requirements." *Id.* at 16.

[20] *See also id.* at 38, n. 119. ("[The] FBI does not log the number of U.S. person query terms conducted at the assessment and pre-assessment stages and thus, the Board is unable to indicate the exact numbers of searches occurring at this stage. In a response by FBI to the Board's request for further information on the numbers, FBI noted that it 'does not have statistics on how many . . . queries were conducted at the assessment stage versus the predicated investigation stage' and that it 'does not have the ability at this time to track the number of unique query terms.'"(citing Fed. Bureau of Investigation, *Responses to May 4, 2022 Written Questions Submitted by PCLOB to FBI*, at 15 (Sept. 9, 2022); Fed. Bureau of Investigation, Attachment B – *Counting U.S. Person Queries*, at 2).

Put simply, as the procedures stand now, rather than discarding Americans' communications or tightly restricting their use—given the absence of a warrant—the government exploits this loophole. It amasses the communications it collects under Section 702 in databases available to FBI agents around the country, who deliberately perform searches for the communications of Americans. The procedures do not require a warrant—or even high-level executive-branch approval—before agents can go looking for an American's private emails or phone calls. *See* PCLOB 2023 Report at 100, 108-115 (discussing FBI procedures). These warrantless queries are designed to extract communications that the government *knows* are protected by the Fourth Amendment. Even if the Constitution permits the government to target foreigners abroad, it does not permit this end-run around Americans' Fourth Amendment rights.

Thus, even if the government did not initially target a U.S.-person such as Mr. Chhipa, if Mr. Chhipa corresponded with a foreign target of 702 surveillance, his data and communications would be swept up in the collection. The FBI can, and would, then query its 702 database for Mr. Chhipa's identifiers and view all of his warrantlessly-amassed content. As discussed in more detail *infra* Part II §E, the Second Circuit has viewed querying Section 702 content as a separate Fourth Amendment event.

Unless compelled to disclose it, only the FBI would know whether any of that 702-acquired data was later used to form the basis for a traditional FISA application or in a search warrant. Even then, though, the FBI has stated that it

does not keep track of whether data from Section 702 queries has been used. *See* PCLOB 2023 Report at 114. "While the government keeps records that enable it to fulfill its notice obligations under Section 1806(c) and 1881e(a), and the government also keeps records of all U.S. person queries as required by Section 1881(f)(1), the government does not systematically track when or whether particular Section 702 information was identified through a U.S. person query. Thus, the government is unable to identify how many times it has used, as part of a criminal investigation or prosecution, evidence that was identified through a U.S. person query specifically. Nor is the government able to identify any instance in which it has used evidence identified through a U.S. person query in a criminal investigation or prosecution." *Id.*

C. Surveillance under Section 702 has been rife with abuse against U.S.-persons as documented by the FISC itself.

There is a profound mismatch between the government's justification for this warrantless surveillance and the way it actually uses the wealth of private emails and phone calls it obtains. "[S]ince at least 2018, the FISC has expressed concern over FBI's query compliance record… For a number of years, these incidents have overwhelmingly involved FBI query compliance incidents." PCLOB 2023 Report at 48 (citations omitted).[21]

[21] According to the PCLOB 2023 Report (at 143), "[w]hile reported compliance incidents at CIA and NCTC have remained close to zero, FBI's reported compliance incidents have numbered in the thousands or tens of thousands, depending on the year… In 2022, the government suspended reporting this rate…."

In its 2018 opinion, FISC stated that "[b]eginning in October 2016, while the 2016 Certifications were pending before the FISC, the government reported that NSA had violated that querying prohibition much more frequently than had been previously disclosed." *Redacted*, 402 F. Supp. 3d at 56. The 2018 FISC opinion explained that "[s]ince April 2017, the government has reported a large number of FBI queries that were not reasonably likely to return foreign-intelligence information or evidence of crime. In a number of cases, a single improper decision or assessment resulted in the use of query terms corresponding to a large number of individuals, including U.S. persons." *Id.* at 76. The FISC then went on to summarize 78,457 problematic FBI queries. *See id.* at 76-79. The 2018 Opinion further identified 57,000 queries as "potentially non-compliant," *id.* at 77, and multiple instances of the FBI querying Section 702 data on individual people for personal reasons. *See id.* at 77-78.

The FISC expressed concern with the FBI's lack of oversight, stating "given the limitations on the oversight of FBI querying practices, it appears entirely possible that further querying violations involving large numbers of U.S.-person query terms have escaped the attention of overseers and have not been reported to the Court." *Id.* at 79-80. As to the FBI's querying policies, the FISC explained, that the "policy decisions may well help FBI personnel work efficiently and 'connect dots' to protect national security, but they also create an environment in which unduly lax applications of the Section 702 querying standard are more likely to occur" and that "it appears that the government may interpret the FBI querying standard

more leniently than its language fairly conveys." *Id.* at 80-81 (internal citations omitted).

Overall, the FISC found "that the FBI's Section 702 minimization procedures, as they have been implemented, are not consistent with the requirements of Section 1801 (h)(1) and (h)(3), or the Fourth Amendment." *Id.* at 82. Specifically,

> The Court regards the privacy interests at stake as substantial. As described above in Part IV.C.3, the FBI has conducted tens of thousands of unjustified queries of Section 702 data. Based on the information available – *e.g.*, queries for [redacted] and for persons with access to FBI facilities – it appears that many subjects of those queries were U.S. persons. Beyond that, it is difficult on the record before the Court to assess to what extent U.S.-person information was returned and examined as a result of those queries. At a minimum, however, the reported querying practices present a serious risk of unwarranted intrusion into the private communications of a large number of U.S. persons.

Id. at 87.

Although acknowledging that the analysis inherently requires balancing privacy intrusions against national security concerns, the FISC held that "[h]ere, there are demonstrated risks of serious error and abuse, and the Court has found the government's procedures do not sufficiently guard against that risk[.]" *Id.* Therefore, "[t]he Court accordingly [found] that the FBI's querying procedures and minimization procedures are not consistent with the requirements of the Fourth Amendment." *Id.* at 92. The FISC granted some of the government's requested

certificates, and denied others. It ordered a series of additional requirements to address the issues. *See id.* at 92-121,134-38.

Just two years later the FISC continued to express dissatisfaction with the FBI's practices. In a November 2020 opinion, the FISC stated that it "the Court continues to be concerned about FBI querying practices involving U.S.-person query terms." *FISC Opinion*, Nov. 18, 2020 at 39 (hereinafter "2020 FISC Opinion").[22] The FISC explained that "the FBI's failure to properly apply its querying standard when searching Section 702-acquired information was more pervasive than was previously believed." *Id.* The FISC found that the FBI committed "widespread violations" of the querying standard. *See id.* at 44. FISC also found abuses of the bulk querying features. Specifically, "[t]he failure to require a written justification for a bulk query involving a U.S.-person query term is particularly concerning given the indiscriminate nature of such queries. *Id.* at 50.

In 2021 problems persisted. The opening line of a September 2021 FISC Order states: "This Order responds to compliance problems regarding the FBI's querying of unminimized information obtained under the Foreign Intelligence Surveillance Act (FISA)…." *FISC Order In Response to Querying Violations* at 1 (2021)(hereinafter "2021 FISC Opinion").[23] The order, drafted by a new Chief Judge, detailed the prior abuses by the FBI discussed above and then stated, "It is now

[22]https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf

[23]https://www.intel.gov/assets/documents/702%20Documents/declassified/21/FISC_Sept2_2021_Order_In_Response_To_Querying_Violations.pdf

apparent that such violations continue and that a common understanding of the querying standard still eludes the FBI and NSD. The FISC explained that "[i]n the reporting period covering November 2020 to December 2021, non-compliant queries related to civil unrest numbered in the tens of thousands." *Id.* at 150-51.

The FISC stated that "[t]he most acute concerns, however, are that the Government is of two minds about what the querying standard means in practice, and that the agency charged with implementing it adheres to an unreasonably lenient interpretation." 2021 FISC Opinion at 9. Therefore, "[a]s long as those circumstances persist, remedial measures can be expected to have only limited effect." *Id.*

One of the issues addressed was compliance with Section 702(f)(2) which "requires the FBI in certain circumstances to obtain approval from the FISC before accessing the contents of communications acquired under Section 702." *Id.* at 10. The opinion noted that "[t]he Foreign Intelligence Surveillance Court of Review has observed that Section 702(f)(2) appears to be intended to address compliance with the Fourth Amendment, and specifically the concern that the foreign intelligence exception to the Fourth Amendment's warrant requirement might not apply in everyday criminal investigations unrelated to national security and foreign intelligence needs." *Id.* (cleaned up). The FISC then explained that "[t]he government has never brought an application to the FISC under Section 702(f)(2). It has, however, reported a number of violations of this provision." *Id.*

FISC ultimately held that "[t]he problems relating to FBI querying practices are substantial and persistent." *Id.* at 13. And a "[f]ailure to correct them would call into question the continued validity, as implemented, of the FBI SMPs for Title I and Title Ill and the FBI BR SMPs, as well as the ability of a FISC judge to find the FBI's Section 702 procedures, as implemented, to be consistent with statutory and Fourth Amendment requirements," and that the remedial measure thus far have not been sufficient. *Id.* at 13-14 (emphasis added). The FISC then ordered the government to submit a series of reports to answer to this issues.

Despite all of these rebukes and additional requirements, a subsequent FISC Opinion noted that the government continued to report significant querying violations, *see FISC Memorandum Opinion and Order*, April 21, 2022 at 26 (hereinafter 2022 FISC Opinion).[24] The FISC explained that "[s]ince the Court issued the Querying Violations Order, the government has reported additional, significant violations of the querying standard…." *Id.* at 28.

In total, the internal audit of the FBI "and NSD's follow-on examination, the government reported in excess of 278,000 non-compliant FBI queries of raw FISA-acquired information." *Id.* at 31. The FISC concluded that "[a]cross the FBI, the government has reported queries of raw FISA-acquired information as part of routine baseline checks in order to determine whether there was any information regarding the subject [of the query] in FBI holdings, without a specific factual basis

[24] Available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf

to believe the query was reasonably likely to return foreign intelligence information or evidence of crime" *Id.* at 33 (cleaned up).

In response to the government's proposed remedial measure, the FISC explained that "[w]ith these revisions, there are no real concerns about whether, *as written*, the querying provisions of the FBI's procedures comport with statutory minimization and Fourth Amendment requirements. The real concerns have always centered on the querying provisions *as likely to be implemented* by the FBI, in view of the repeated querying violations." 2022 FISC Opinion at 36 (emphasis in original). The FISC characterized the querying compliance problems "persistent and widespread." *Id.* at 49.

Particularly relevant to an individual criminal case, the FISC acknowledged that regardless of the procedures formulated, it is an imperfect system and errors would still be present. Specifically, the FISC stated, "[p]erfect implementation is unrealistic[.]" *Id.* at 67. However, the FISC is not tasked with evaluating an individual query for an individual case, but instead to evaluate the FBI's procedures as a whole. Thus, FISC concluded that "some potential for error is not a sufficient reason to invalidate procedures as unreasonable. Nevertheless, if the scope and pervasiveness of FBI querying violations were to continue unabated, they would present greater statutory and Fourth Amendment difficulties in the future." *Id.* (internal quotations and citations omitted).

D. The government's collection of 702 material on Mr. Chhipa is obvious and the government does not deny it.

We know in this case from the public documents alone, that at the time the government was investigating Mr. Chhipa it was also investigating foreign citizens for suspected connections to terrorist organizations. It is unrealistic to think that the government was *not* conducting 702 surveillance against the British person referenced in the Affidavit in Support of the Criminal Complaint. *See* ECF No. 4. These foreign citizens would have undoubtedly been the target of Section 702 surveillance as those are the very people Section 702 is intended to cover. According to the government, Mr. Chhipa communicated with those foreign targets. Thus, even if the government was not investigating Mr. Chhipa at that time, his communications would have been swept up in the collection of Section 702 material targeting the foreign nationals.

Mr. Chhipa's alleged communication with foreign nationals is not the only intercepted communication produced in discovery, however. Also produced were intercepted and recorded phone calls between Mr. Chhipa and other U.S. Persons based domestically such as his family. The government will not disclose the authority under which these calls were captured, thus it is almost surely through a FISA application claiming that Mr. Chhipa was acting as an agent of a foreign power. The information to form the probable cause for this claim in the FISA application had to have been generated from somewhere. The most obviously place is from the previously-collected Section 702 information involving Mr. Chhipa.

As stated by the FBI itself, investigations do not begin with FISA surveillance. Rather, as in other cases, the government's FISA surveillance was

undoubtedly the product of a pre-existing investigation. See *Testimony of James Baker*, former FBI General Counsel, at 68-71 (FISA surveillance "is not typically the first thing[] that is done in an investigation. You build up to that point. You collect other information . . . and develop your probable cause.")[25] The other collection of information is at least in part Section 702 data. "The FBI [] will query previously acquired information from a variety of sources, including Section 702 when it 'opens new national security investigations.'" *United States v. Hasbajrami*, 945 F.3d 641, 648 (2d Cir. 2019)(citing a 2014 PCLOB Report on Section 702 surveillance).

In fact, the FBI uses its Section 702 database as a "search engine for routine use." PCLOB 2023 Report at 191-92. As the PCLOB explained, "the "FBI queried community leaders and religious leaders, as well as everyday Americans who came into an FBI field office to provide a tip. The fact that FBI received the information and immediately used a known U.S. person identifier to search the Section 702 database either to verify or refute the information despite the lack of any apparent connection to foreign intelligence presents a significant privacy harm. The behavior indicates that FBI has treated Section 702 databases essentially as a search engine for routine use." *Id.*

In this case, it is clear that after the FBI closed its investigation in 2018, it was still surveilling Mr. Chhipa. One of the search warrants indicates the investigation was reopened based on social media posts that the FBI attributed to

[25] Executive Session, Committees on Judiciary and Government Reform & Oversight, U.S. House of Representatives (Oct. 3, 2018), https://s3.documentcloud.org/documents/5805759/Baker-Transcript.pdf.

Mr. Chhipa, yet that same search warrant does not detail how the FBI would have connected any particular social media account to Mr. Chhipa. *See* Def.'s Exhibit 3 at 4. In fact, it appears quite obvious in Def.'s Ex. 1 (at 4, 6) that the FBI conducted a backdoor query on Mr. Chhipa in 2019 before the full investigation was reopened. An FBI report states (through redactions) that, after coming across some public posts that the FBI found questionable on March 15, 2019, it conducted a search to identify the user of carl johnson facebook account which it states it identified as Mohammed Chhipa. *See id.* at 4. The FBI then stated:

[redacted] On 03/20/2019, WFO became aware of other information related to Chhipa [redacted], beyond the scope of this document.

[redacted] On [redacted] WFO re-opened FI on Chhipa.

Id. at 6. Thus, the FBI gathered information through undisclosed means to determine the identity of a U.S.-person prior to an investigation even being opened.

Perhaps more conclusively, in the FBI report dated March 2019, Def.'s Ex. 2 at 4-10 the FBI listed out (at 9) "facilities" (phone numbers and email addresses) for different platforms and user IDs without yet having received returns from the service providers identifying those "facilities." *See* Def.'s Ex. 3 at 5 (showing April and May 2019 for the returns). For example, the FBI agent apparently viewed the carl johnson facebook account through the normal course on the open internet in March 2019. According to the search warrant, Def.'s Exhibit 3 at 5, the "facebook records received by the FBI in March 2019" associated that facebook account with an email address, wanderer377@gmail.com. Indeed, this is precisely the information

in that return generated on March 19, 2019. *See* Def.'s Ex. 5. Yet, on March 20, 2019 the government issued a grand jury subpoena for a completely different email account, azharc37@gmail.com, with no indication as to how that account came to the attention of the FBI, let alone that it was associated with Mr. Chippa. *See* Def.'s Ex. 4. Further, a March 2019 FBI report (Def.'s Ex. 2 at 9-10) includes, multiple accounts and identifiers as associated with Mr. Chhipa with no indication as to how the FBI would have associated these with Mr. Chhipa.

But even if there weren't these gaps in the information timeline, just simply using the term "facilities" which is known to correspond to "selectors" for Section 702-queries, *see* PCLOB 2023 Report at 3 ("Selectors may be communications facilities that are assessed to be used by the target, such as the target's email address or telephone number") and saying that it "searched" them (Def.'s Ex. 2 at 9) gives rise to a strong indication of a backdoor query. That the identification of "facilities" is then followed by "targeting" in the same report is an even more clear signal that this information was part of a backdoor 702-query on a U.S. person, Mohammed Chhipa. *Id.* at 9-10.

A final indication are the numerous passive and vague references in the search warrants and other legal processes that appear designed to conceal the source of the FBI's information.[26] This further suggests the government's use of

[26] In search warrant, 19-sw-1102, 8/2/19 it states, "*Investigation has revealed* that Chhipa created at least 12 Facebook accounts between 2008 and 2019" and "*FBI investigation has also determined* Chhipa created a channel in an encrypted application." In search warrants 19-sw-1122 and 19-sw-1123, 8/16/19 Search of 2 CDs and Anticipatory Search of Android Cellular Device, and in search warrant 19-sw-1129, 8/19/19 Search of MP3 player it states "in connection with the Aug 2

Section 702 material. *See e.g.* John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013;[27] Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, Wash. Post, Feb. 22, 2015.[28]

Mr. Chhipa was subjected to multiple kinds of intrusive surveillance. For exampled, agents searched his email communications, logged his internet browsing,

---

search" of Mr. Chhipa's home the FBI located a July 2019 encrypted message. These search warrants also state that the FBI "*received additional information*" regarding Mr. Chhipa's purchase of a bus ticket. In §2702 request to Text Now on 8/22/2019 it states, "The FBI conducted a search warrant of the target's residence and know that the target has multiple Email accounts to include [email address] which appears to match user CS123 tied to TextNow. Though *appropriate legal process* we have additionally identified [phone number] to have been used by the target during the aforementioned timeframe which we have identified as a textnow number…." In search warrant 20-sw-1559, 10/22/2020, Search of two Facebook Accounts it states "On May 16 2019 *a foreign government provided the FBI with information* that indicated Chhipa was using Facebook account Nu'man Ibn Muqrin Al-Muzanee." In search warrant, 21-sw-233, 4/14/2021, it states twice, "*Based on other investigative steps* taken during the course of the investigation the FBI was already aware of [two Telegram accounts]." In §2702 request to Google on 4/28/23, it states that a redacted agency indicated to redacted that one of the potential targets had a business located near this attorney. In §2702 T-Mobile request and supplemental request on 4/28/23, it states "*Based on the investigation* Chhipa is believed to utilize T Mobile telephone numbers [number] and [number]." In search warrant 23-sw-236, 4/30/2023 it states twice that *information was provided by a foreign government*. In §2702 Meta request on 5/1/2023 it states that "*Based on the investigation* Chhipa is believed to utilize Instagram accounts that are subscribed to the following email addresses." A separate §2702 request this same day states, "*Chhipa is believed* to utilize an Instagram account with the following username and UID." In §2702 request to Verizon 5/2/2023 it states, "*Based on the investigation Chhipa is believed* to have access to the vehicle mentioned below…." (emphasis added in all).

[27] https://www.reuters.com/article/idUSBRE97409S/

[28] https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html

recorded his telephone calls, tracked his physical location, and examined his financial transactions. Some of the government's surveillance in this case was conducted pursuant to FISA orders, but certainly not all of it.

Given that the probable cause for the traditional FISA application had to have originated from somewhere; the fact that the FBI has been known to have concealed and/or misrepresented information in a FISA application in the past; the fact that the FBI queries its 702 database whenever it opens a national security investigation and uses that database as a search engine for routine use; that the legal processes the defense does possess in discovery contain what appear to be intentionally vague references; the gaps in the information timeline; the cryptic, redacted references to obtaining additional information outside the scope of the report in the early stages of reopening an investigation; and the reference to "facilities" identified before returns were provided that is then related to "targeting," makes the collection of Section 702 material on Mr. Chhipa obvious. When asked, the government does not deny it. Nor does the government deny using other surveillance programs to collect information on Mr. Chhipa. The government's only response is that Mr. Chhipa has received the notices he is entitled to.

In *Hasbajrami*, 945 F.3d at 648, the defendant first received a traditional FISA notice. After he pled guilty and was serving his sentence, "the government provided him with a supplemental letter disclosing, for the first time, that some of the evidence it had previously disclosed from FISA surveillance was itself the fruit of earlier information obtained without a warrant pursuant to Section 702 of the

FISA Amendments Act[.]" *Id.* The Second Circuit opined that "[t]he government's provision of notice in this case was likely in response the Solicitor General's assertion, at oral argument before the Supreme Court in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), that prosecutors would provide notice to defendants in cases where evidence was derived from Section 702 surveillance. *See Charlie Savage, Door May Open Challenge to Secret Wiretaps*, N.Y.Times (Oct. 17, 2013).[29] While the government's policy prior to *Clapper* was not to provide notice of Section 702 surveillance, it began reviewing cases and providing supplemental notice in 2013." *Id.* The district court then allowed the defendant to withdraw his plea and file a second motion to suppress based on the government's new notice of the Section 702 evidence. *See id.*

The government's decision to provide the supplemental notice to the defendant of additional FISA information in *Hasbajrami* thus appears to be based, not on any provision of law, but instead on an office policy. It is unknown whether this policy still exists, or whether it has changed. The statistics suggest that this notice may have been a short-lived policy: Only seventeen defendants have been provided with a Section 702 notice in the last four years despite the billions of communications captured. It is unrealistic to think that in the face of this massive collection only seventeen U.S.-person have had their information used for a domestic criminal case, especially since the Carter Page revelations and documented misuses of FISA and FAA. The Office of the Director of National

[29] https://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html

Intelligence has self-reported well over 3 million U.S.-person queries conducted by the FBI over the last three years, *see supra* Part II §B, yet the ODNI reports on having filed FISA Notices in just *seventeen criminal cases* in 2020-2022. *See* ODNI 2023 Statistical Transparency Report at 34.

Of course knowing whether Section 702 information was collected, retained, and queried, or used in any capacity to investigate Mr. Chhipa is critical to being able to evaluate the Constitutional implications and challenges he might have to the fruit of that collection. The government cannot have it both ways. It cannot affirmatively state that the information was not "used" for the purposes of a criminal prosecution, but then turn around and say it does not track whether Section 702 information is used in a criminal prosecution when it comes oversight of the programs. Either the government has tracked it and knows it was used or not used; or the government does not track it in which case the government should be compelled to review all the steps from all the individuals who may have been involved in collecting or searching Mr. Chhipa's information, and to disclose the findings to cleared defense counsel so defense counsel may further assert Mr. Chhipa's bases for suppression.

In any event, although his information is necessary for Mr. Chhipa to be able to adequately articulate the specifics of his ground for suppression, the definition of "aggrieved person" itself under 50 U.S. Code § 1801(k) does not require that the government file a notice of having collected Section 702 material to allow Mr. Chhipa to move to suppress its contents and its fruits. § 1801(k) simply states that

an "aggrieved person" is a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance. In this case, Mr. Chhipa was obviously the target of electronic surveillance beyond traditional FISA and therefore may move to suppress the collected material and the fruits derived thereof under 50 U.S.C. §1806(e) (applying to Section 702 through 50 U.S.C. 50 U.S. Code § 1881e(a)(1)).

E. The Section 702 collection and search of Mr. Chhipa's communications and data violates his constitutional protections.

i. Section 702 surveillance violates the warrant requirement.

Under the Fourth Amendment, Americans have a protected privacy interest in the contents of their communications, including their telephone calls and emails. *See United States v. U.S. Dist. Court* (Keith), 407 U.S. 297, 313 (1972); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The government therefore needs a warrant to search and seize these communications. Searches conducted without a warrant are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967).

Section 702 does not require the government to obtain a warrant based on probable cause prior to collecting the communications of Americans, nor does it impose any comparable requirement after the fact. *See* PCLOB 2023 Report at 179 ("Section 702 targeting decisions lack the checks that are part of traditional FISA or criminal electronic surveillance."). The government's collection, searching, and use of these communications is therefore presumptively unconstitutional. Moreover, no

exception to the warrant requirement exists that could justify such a sweeping program of suspicionless searches. As the PCLOB stated, "[b]y collecting the contents of communications, even though the U.S. persons are not the target, surveillance conducted under Section 702 acquires information that involves private content in which the U.S. persons have an expectation of privacy. This includes text and audio communications generated by the user. The collected material can therefore be highly personal and sensitive, capturing exchanges with loved ones, friends, medical providers, academic advisors, lawyers, or religious leaders, among others. This material can also provide great insight into an individual's whereabouts, both in a given moment and in patterns over time. Further, the knowledge that the government can gather this sort of content can have a chilling effect on speech." PCLOB 2023 Report at 179.

There is no foreign intelligence exception to the warrant requirement. Courts recognize an exception to the warrant requirement only "in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). The mere fact that the government conducts this surveillance to acquire foreign-intelligence information does not render the warrant and probable-cause requirements unworkable. In *Keith*, the Supreme Court expressly rejected the government's argument that intelligence needs justified dispensing with the warrant requirement in domestic surveillance cases. 407 U.S. at 316-21. That logic applies with equal force to

surveillance directed at targets with a foreign nexus—at least when that surveillance sweeps up Americans' communications (as Section 702 surveillance does), and is conducted inside the United States (as Section 702 surveillance is).

The Supreme Court has never recognized a foreign-intelligence exception to the warrant requirement. But even if such an exception exists, it is not broad enough to render Section 702 surveillance constitutional. Courts have approved narrow modifications to the probable-cause requirement when considering individualized surveillance under FISA, but only where the surveillance in question was (1) directed at foreign powers or their agents; and (2) predicated on an individualized finding of suspicion. *See, e.g., United States v. Duggan*, 743 F.2d 59, 73-74 (2d Cir. 1984); *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *In re Sealed Case*, 310 F.3d 717, 720 (FISCR 2002).

Section 702 contains no such limitations. The surveillance is not confined to "foreign powers or agents of foreign powers reasonably believed to be located outside the United States"—a limitation the FISCR deemed critical in analyzing similar surveillance. *See In re Directives*, 551 F.3d 1004, 1012-16 (FISCR 2008). Instead, under Section 702, the government may target *any* non-citizen outside the United States to acquire "foreign intelligence information," broadly defined. Moreover, where prior cases required a probable-cause determination by the President or Attorney General, *see, e.g., id.*, under Section 702, targeting decisions have been handed off to an untold number of government analysts. While foreign intelligence

gathering is unquestionably a government interest of the highest order, it does not exempt surveillance of Americans from the warrant requirement.

In this case, the government's obvious collection and backdoor querying of Mr. Chhipa's communications violates the Fourth Amendment because the statute itself is unconstitutional and because its application resulted in an unlawful search and seizure. The fruits of this search, including any subsequent traditional FISA material, should be suppressed from the government's use at trial.

ii. Even if initial collection was not unconstitutional, the FBI's subsequent querying of the information using Mr. Chhipa's identifiers is a separate Fourth Amendment event and violates its protections.

The government has in the past, and would likely argue in this case, that since the initial collection may have been lawful against a foreign citizen, the subsequently query of that collection for Mr. Chhipa's identifiers likewise conforms to the Fourth Amendment's requirements. The Second Circuit has rejected this argument, and so too should this Court. As the Second Circuit explained:

> We do not find that logic persuasive. Storage has little significance in its own right: the lawfully-collected communications, even of United States persons, continue to serve the same foreign intelligence purpose in the continued surveillance of a foreign operative, whether his interlocutor is a United States person or a citizen and resident of some other country. The material is justifiably retained, not to keep tabs on a United States person, but to keep tabs on the non-United States person abroad who has been targeted. But querying that stored data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable.

Hasbajrami, 945 F.3d at 670.

The Second Circuit then explained that "[]it is true that the FBI does not need an additional warrant to go down to its evidence locker and look through a box of evidence it collected from a crime scene. But lawful collection alone is not always enough to justify a future search." *Id.* The court compared 702-collected data with data stored in a cell phone as in *Riley v. California*, 573 U.S. 373, 401 (2014), stating that "the Supreme Court held that a warrant was necessary to search a cell phone, even when that cell phone was lawfully seized pursuant to a search incident to a lawful arrest." *Id.* The Second Circuit explained,

> [I]f such a vast body of information is simply stored in a database, available for review by request from domestic law enforcement agencies solely on the speculative possibility that evidence of interest to agents investigating a particular individual might be found there, the program begins to look more like a dragnet, and a query more like a general warrant, and less like an individual officer going to the evidence locker to check a previously-acquired piece of evidence against some newfound insight.

Id. at 671. The Second Circuit summed up this analysis by stating:

> The Supreme Court has expressed increasing concern about the interaction between Fourth Amendment precedent and evolving government technological capabilities. *Riley* rested in part on the fact that "[c]ell phones ... place vast quantities of personal information literally in the hands of individuals." 573 U.S. at 386, 134. "A search of the information on a cell phone [therefore] bears little resemblance to the type of physical search considered" in past cases. *Id.*; *see also Ganias*, 824 F.3d at 217-18 (noting privacy implications of expansive technology and data storage). And in *Carpenter*, the Court concluded that a warrant (or a valid substitute) was required to acquire cell-site records, even though they were stored by a third party and under traditional Fourth Amendment doctrine a cellphone user would not have an expectation of privacy in such information.

Id.

Additionally, the Second Circuit addressed the practical implications of querying Section 702-acquired material:

> As a practical matter, querying is problematic because it may make it easier to target wide-ranging information about a given United States person at a point when the government knows it is investigating such a person. Section 702 forbids the government from targeting a non-United States person as a backdoor way of targeting a United States person. 50 U.S.C. § 1881a(b). But, as detailed above, in the course of its intelligence gathering operations, the NSA may have collected all sorts of information about an individual, the sum of which may resemble what the NSA would have gathered if it had directly targeted that individual in the first place. To permit that information to be accessed indiscriminately, for domestic law enforcement purposes, without any reason to believe that the individual is involved in any criminal activity and or even that any information about the person is likely to be in the database, just to see if there is anything incriminating in any conversations that might happen to be there, would be at odds with the bedrock Fourth Amendment concept that law enforcement agents may not invade the privacy of individuals without some objective reason to believe that evidence of crime will be found by a search. Treating querying as a Fourth Amendment event and requiring the query itself to be reasonable provides a backstop to protect the privacy interests of United States persons and ensure that they are not being improperly targeted.

Id. at 672.

Finally, the Second Circuit addressed the significance of *who* was querying the data – the NSA or the FBI. The court stated, "FBI queries directed to a larger archive of millions of communications collected and stored by the NSA for foreign intelligence purposes, on the chance that something in those files might contain incriminating information about a person of interest to domestic law enforcement, raise different concerns." *Id.*

The PCLOB also addressed these querying issues as separate Fourth Amendment events. The PCLOB stated, "U.S. person queries present some of the most serious privacy and civil liberties harms." PCOLB 2023 Report at 184. The PLOB further explained:

> FBI's querying practices pose greater threats to privacy because the FBI, as the United States' domestic law enforcement agency, has the ability and the mission to investigate and prosecute Americans for crimes. When an American faces the prospect of criminal investigation and prosecution, their privacy interests are at their highest. Since, as noted, Americans' sensitive communications are incidentally collected under Section 702 even when individuals have no reason to believe that they are in contact with wrongdoers, robust guardrails are needed to protect privacy rights in circumstances where the government seeks to search through those communications.

Id.

In fact, according to the PCLOB, "searches performed before an investigation even begins create one of the greatest threats to privacy and civil liberties." *Id.* This is because "[a]ccording to FBI's Domestic Investigations and Operations Guide, assessments do not require factual predication, but do require an authorized purpose and clearly defined objectives. The pre-assessment stage requires neither. Although Section 702 queries must still meet the query standard, the low thresholds applicable at the pre-assessment stage increase the risk that an individual's private communications will be compiled despite the lack of any basis to suspect the individual of wrongdoing. Further, even though the communications identified through a database query have already been collected, compiling all of a specific individual's communications contained in the database and surfacing them

for review by an agent constitutes a privacy invasion that requires more sufficient justification than is currently provided." *Id.* at 190 (citations omitted).

Thus, even if the government is permitted to surveil foreigners without first obtaining a warrant, it is not entitled to completely bypass the Fourth Amendment rights of Americans like Mr. Chhipa. Rather, the government's reasoning would justify, at most, the warrantless acquisition and querying of foreign-to-foreign communications, in which it says no Fourth Amendment interests are implicated. But instead the government seeks a windfall: the ability to retain, use, and deliberately query its massive Section 702 databases for the emails of known Americans, without ever satisfying bedrock Fourth Amendment requirements.

In this case, it is clear that Mr. Chhipa was subject to a backdoor query "before [the] investigation even beg[an]" which "create[s] one of the greatest threats to privacy and civil liberties." *Id.* The FBI noticed some questionable facebook posts on March 15, 2019. *See* Def.'s Ex 1. at 4. On March 20, 2019, the FBI reported that it "became aware of other information related to Chhipa [redacted] beyond the scope of this document." *Id.* at 6. Also on March 20, 2019, the government sent a grand jury subpoena to google for information on an email address that the government would not have known about at that point according to its own documents. *See* Def.'s Ex. 3 at 5; Def.'s Ex. 5. Then, "On [redacted] WFO [FBI Washington Field Office] re-opened FI [full investigation] on Chhipa." Def.'s Ex. 6.

a) The warrant requirement applies to a query of 702-collected data of a U.S. person.

To the extent the government claims it is unable to avoid seizing Americans' communications in the first place, reasonableness requires that it provide comparable Fourth Amendment protection to Americans after its initial seizure. At a minimum, agents must obtain individualized judicial approval at the point when they seek to query or use an American's communications. Because Section 702 has no such post-seizure limitations,[30] any such surveillance of Mr. Chhippa was unreasonable.

In 2013, the President's Review Group concluded that a warrant requirement should be imposed, and the House of Representatives passed a bill that would prohibit the retention and use of Americans' communications. *See* President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* at 183 (Dec. 12, 2013);[31] H.R. 4870, 113th Cong. § 8127 (2014); H.R. 4870, 113th Cong. § 8127 (2014). Accordingly, the government must, at a minimum, obtain a warrant when it deliberately seeks to use or search for the communications of Americans. Especially in the context of electronic searches, courts have frequently required the government to obtain a warrant after its initial seizure or search. *See, e.g., Riley v. California*, 134 S. Ct. 2473, 2493 (2014) (requiring government to obtain a warrant before searching cell phone

---

[30] *See* PCLOB 2023 Report at 184 ("Except in the very limited circumstances… government personnel are not required by Section 702 to make any showing of suspicion that the U.S. person is engaged in any form of wrongdoing prior to using a query term associated with that specific U.S. person.")

[31] https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

lawfully seized incident to arrest); *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (requiring government to obtain a warrant before conducting new search of lawfully seized computer hard-drive). *See United States v. Loera*, 923 F.3d 907, 922-23 (10th Cir. 2019); (In cases concerning computer hard-drive searches in which data is often intermingled the courts recognize the importance of post-seizure restrictions, allowing a search only for the particular information authorized by the probable-cause warrant).

Strong post-seizure restrictions are especially critical under Section 702 given the breadth of the collection and the absence of traditional Fourth Amendment safeguards at the outset. Here, they would also answer one of the government's principal objections: that it would be impractical to obtain a warrant beforehand, because it cannot know whether surveillance directed at a given foreigner will sweep up protected communications involving Americans. But that fact—even if true in some instances—does not excuse the government from obtaining individualized judicial approval when it later seeks to use communications that it knows are protected. As the PCLOB stated, "it is important that the rules for U.S. person queries should not enable law enforcement to rely on this practice to convert a foreign intelligence collection authority into a domestic law enforcement tool, and thereby evade otherwise applicable privacy safeguards." PCLOB 2023 Report at 189. Thus, the PCLOB recommended that Congress "raise the standards for conducting U.S. person queries to ensure sufficient protection for Americans' privacy rights." *Id.*

Finally, just recently, a bipartisan effort was launched in the United States Senate to require the FBI to obtain a search warrant before it queries U.S.-person search terms. In March 2024, Senators Dick Durbin and Kevin Cramer, filed an amendment to the FISA Reauthorization Bill that would require the government to obtain a warrant from the Foreign Intelligence Surveillance Court (FISC) before reviewing the contents of Americans' private communications that get swept up in Section 702 surveillance. *See* U.S. Senate, Committee on the *Judiciary, Durbin, Lee Introduce Bipartisan SAFE Act to Reform FISA Section 702* (March 14, 2024).[32] Senator Durbin explained that "[i]f the government wants to spy on my private communications or the private communications of any American, they should be required to get approval from a judge, just as our Founding Fathers intended in writing the Constitution." Ellen Nakashima et al, *Congress extends controversial warrantless surveillance law for two years*, Washington Post (April 20, 2024).

b) The current procedures for querying the 702-collected data of U.S. Persons is unreasonable.

Regardless of whether the warrant requirement applies, "the ultimate touchstone of the Fourth Amendment is reasonableness," *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006), and the government's purposeful exploitation of Americans' communications in this manner is unreasonable. The constitutionality of electronic surveillance regimes depends not just on limitations on initial collection but also on the restrictions on later retention and use. Because Section

[32] https://www.judiciary.senate.gov/press/releases/durbin-lee-introduce-bipartisan-safe-act-to-reform-fisa-section-702

702 is extremely permissive at the outset—allowing the broad, continuous collection of billions of communications—strong post-seizure restrictions on the use of this information are critical to the Fourth Amendment analysis.

In assessing such restrictions, the government's justification for its initial search matters. When the government justifies warrantless surveillance by asserting that its foreign targets lack Fourth Amendment rights, its subsequent use and querying of Americans' communications without any individualized judicial approval is unreasonable. *See In re Directives*, 551 F.3d at 1015 (finding warrantless surveillance of foreigners reasonable only after the government represented that it was not amassing databases of Americans' incidentally collected communications); *see generally Terry v. Ohio*, 392 U.S. 1, 19 (1968) ("The scope of the search must be strictly tied to and justified by the circumstances which rendered its initiation permissible.").

Because of the "inherent dangers" and overbreadth of electronic searches, courts have long looked to post-seizure limitations when analyzing the reasonableness of surveillance. *Berger v. State of N.Y.*, 388 U.S. 41, 60 (1967). For example, in *Berger*, the Supreme Court faulted New York's eavesdropping statute in part because it did not limit the surveillance to particular conversations, but instead permitted the retention and use of "any and all conversations" of the state's targets; it did not meaningfully constrain the duration of surveillance; and it did not provide for after-the-fact notice to those monitored. *See id.* at 58-60. Drawing heavily on *Berger*, the Tenth Circuit upheld the constitutionality of video

surveillance in *United States v. Mesa-Rincon*, 911 F.2d 1433, 1439-1441 (10th Cir. 1990), holding modified by *United States v. Castillo-Garcia*, 117 F.3d 1179 (10th Cir. 1997)—but only after insisting on "precise" minimization rules that prevented the government from continuously and indiscriminately recording private activities. *See Tortorello*, 480 F.2d at 772-73, 783-84 (Title III).

Likewise, courts considering the reasonableness of foreign-intelligence surveillance have relied on FISA's minimization procedures, which regulate how the government may retain, use, and disseminate the information it obtains. *See In re Sealed Case*, 310 F.3d at 740. These cases belie the government's claim that so long as its targeting of foreigners was "lawful" at the outset, the Fourth Amendment has nothing to say about its subsequent querying or use of Americans' communications. *See also* PCLOB 2023 Report at 186 ("While the government takes seriously the prohibition against reverse targeting—which bans targeting a person outside the United States as a pretext to target a known person reasonably believed to be located in the United States—its approach to U.S. person queries threatens to undermine that critical safeguard for Americans' privacy rights.").

The government's insistence that it can freely exploit Americans' emails and phone calls without further judicial approval is at odds, too, with another line of Supreme Court cases. Because the Fourth Amendment carries a continuing requirement of reasonableness, the government's duties often change as its search or seizure becomes more intrusive. *See Rodriguez v. United States*, 135 S. Ct. 1609, 1614-15 (2015) (traffic stop that was lawful when initiated violated Fourth

Amendment when officer's investigation expanded beyond original justification); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (reasonableness of warrantless drug tests depended on protections against later dissemination of the results); *United States v. Place*, 462 U.S. 696, 709-10 (1983) (a seizure lawful at its inception can nevertheless violate the Fourth Amendment based on agents' subsequent conduct). Even if a warrantless search or seizure is lawful when initiated, reasonableness limits how far agents may intrude on protected interests before they must obtain judicial approval. At the very least, reasonableness requires the provision of safeguards for Americans after the fact. [33]

The mere fact that the government is "targeting" foreigners when it acquires Americans' protected communications is not a valid reason to jettison the safeguards that a warrant would otherwise afford. While post-seizure restrictions could adequately protect the rights of Americans under Section 702, the existing procedures do the opposite. They allow the government to collect Americans' communications on U.S. soil without a warrant. They allow the government to retain those communications for five years by default—and to pool them in massive centralized databases. And they allow agents to conduct queries that deliberately target Americans' communications after they are collected, including for use in criminal investigations. In short, the procedures authorize the very type of intrusion that the Fourth Amendment was designed to guard against.

---

[33] *See* Peter Swire & Richard Clarke, *Reform Section 702 to Maintain Fourth Amendment Principles*, Lawfare (Oct. 19, 2017) https://goo.gl/RHqdND; Geoffre Stone & Michael Morell, *The One Change We Need to Surveillance Law*, Wash. Post (Oct. 9, 2017) http://wapo.st/2hZ1xJx.

The collection and subsequent search of Section 702 surveillance and any other surveillance programs in Mr. Chhipa's case violated his Fourth Amendment protections. The fruits of this unlawful surveillance must be suppressed.

III. The underlying FISA applications; notice of Section 702 use and the Section 702 material; and notice of any other intelligence surveillance use and corresponding material should be disclosed to defense counsel.

A. Disclosure of FISA and FAA materials to the defense pursuant to §1806(f)

Both traditional FISA and FAA are governed by 50 U.S.C. §1806(f) when it comes to use of information. *See* 50 U.S. Code § 1881e (explaining that information acquired from an acquisition conducted under section 1881a shall be deemed "electronic surveillance" for purposes of §1806). According to FISA's legislative history, disclosure may be "necessary" under §1806(f) "where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" *Belfield*, 692 F.2d at 147 (quoting S. Rep. No. 701, 95th Cong., 2d Sess. 64 (1979)); *see, e.g.*, *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (same); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (same). Here, these factors require disclosure.

The defense requires this information to determine whether the FISA applications were tainted by other unconstitutional searches. *See Wong Sun v.*

United States, 371 U.S. 471, 487-88 (1963). This question is enormously complex. While some of the information in the government's FISA application was likely obtained pursuant to Section 702, other information was may have been obtained using other novel or illegal techniques, such as the warrantless collection of cell-site location data or the bulk collection of call records. *See supra* Part I §B.

In this case the FBI monitored numerous social media accounts using multiple undercover employees who at times also assumed more than one online identity. Mr. Chhipa was effectively under investigation fifteen years; from 2008 until he was arrested in 2023. By the time Mr. Chhipa's family calls were intercepted in 2019-2022, the FBI had been surveilling him for roughly ten years and would have needed to support that FISA wiretap application with some information for probable cause. Without access to the FISA applications, however, Mr. Chhipa could not adequately raise any arguments as to the basis for probable cause in that application.

There are ample justifications for disclosure of the FISA applications in this case which would permit defense counsel an opportunity to demonstrate that the requisite probable cause with respect to the issue of knowledge was lacking, that with respect to the defendant, "United States person[s]," the alleged "activities" fell within the protection of the First Amendment and, thus, could not be used as a basis for probable cause in any event, and that the information in the applications was either unreliable or obtained via illegal means. Disclosure would also afford defense counsel an opportunity to identify procedural irregularities.

In addition, counsel for the defendant possess security clearances for this case. The Court therefore could issue an appropriate Protective Order that would provide elaborate protection for classified information, and which would permit such materials to be disclosed to defense counsel but not to the defendant. *See* Classified Information Procedures Act (hereinafter "CIPA"), 18 U.S.C. App. III, at §3.

Thus, while only one court in the history of FISA (*United States v. Daoud*, No. 12 CR 723, 2014 WL 321384, at *2 (N.D. Ill. Jan. 29, 2014))[34] has ordered disclosure of FISA applications, orders, or related materials, *see, e.g.*, *In re Grand Jury Proceedings*, 347 F.3d 197, 203 (7th Cir. 2003) (citing cases), and that district court was overturned, *see United States v. Daoud*, 755 F.3d 479 (7th Cir.), supplemented, 761 F.3d 678 (7th Cir. 2014), disclosure should occur in this case. Indeed, the existence of §1806(f) is an unambiguous declaration that Congress intended for courts to grant disclosure in appropriate cases. If §1806(f) is to be

[34] *Daud* stated: "Assuming that counsel's clearances are still valid and have not expired, top secret SCI clearance would allow him to examine the classified FISA application material, if he were in the position of the Court or the prosecution. Furthermore, the government had no meaningful response to the argument by defense counsel that the supposed national security interest at stake is not implicated where defense counsel has the necessary security clearances. The government's only response at oral argument was that it has never been done. That response is unpersuasive where it is the government's claim of privilege to preserve national security that triggered this proceeding. Without a more adequate response to the question of how disclosure of materials to cleared defense counsel pursuant to protective order jeopardizes national security, this Court believes that the probable value of disclosure and the risk of nondisclosure outweigh the potential danger of disclosure to cleared counsel." 2014 WL 321384, at *2.

rendered meaningful at all, and not be rendered superfluous and entirely inert, it should apply in this case.

The Section 702-acquired data and specifics on the collection, retention, and queries is also necessary. As the FISC found in 2022, "[p]erfect implementation is unrealistic[.]" 2022 FISC Opinion at 67. Especially given this acknowledgment, the defense must be able to assess the technical methods for collection, whether the specific Section 702 targeting, minimization, and querying procedures that applied to Mr. Chhippa communications complied with the Fourth Amendment and FISA—and whether the government adhered to those procedures.

For example, it is now known that while the investigation against Mr. Chhipa was ongoing, in 2018 FISC partially denied the government's requested certificates on its querying procedures based on compliance and Fourth Amendment concerns. *See* 2018 FISC Opinion at 92-121,134-38. Another issue raises specific concerns for Mr. Chhipa's case as well, namely knowing that "compliance incidents have resulted from an analyst in one field office querying Section 702- acquired information using a U.S. person query term in response to a lead from another field office, unaware that the other field office had opened a predicated criminal investigation on the same matter." PCLOB 2023 Report at 147.

This sounds strikingly similar to Mr. Chhipa's situation in which two separate FBI offices were investigating him, and eventually overlapped. If this *was* Mr. Chhipa's case, or even if it is merely similar to Mr. Chhipa's situation, it should

have prompted a 702(f)(2) Order. As multiple sources have reported – the government has never sought a 702(f)(2). Thus, one would not have been issued.

More recently, and also during the period when Mr. Chhipa was being investigated the FISC identified significant problems with the government's backdoor searches of Section 702 data, as well as an array of hundreds of thousands of other violations. *See supra* Part II §C. Without access to these records, the defense cannot adequately challenge the procedure used in this case.

B. Disclosure of FISA and FAA materials to the defense pursuant to §1806(g)

Even if the Court were to decline to find that disclosure of FISA and FAA-related materials to the defense is appropriate under §1806(f), the defense would still be entitled to disclosure of the FISA applications, orders, and related materials under §1806(g), which expressly incorporates the Fifth Amendment Due Process Clause, and provides that "[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure*." 50 U.S.C.§1806(g) (emphasis added). *See also United States v. Spanjol*, 720 F. Supp. 55, 57 (E.D. Pa. 1989) ("[u]nder FISA, defendants are permitted discovery of materials only to the extent required by due process. That has been interpreted as requiring production of materials mandated by [Brady], essentially exculpatory materials").

C. Mr. Chhipa is entitled to official notice of Section 702 and other government surveillance programs used to collect his protected information.

i. The Fourth and Fifth Amendments entitle Mr. Chhipa to notice of the government's surveillance techniques.

Notice of the government's surveillance techniques is essential to Mr. Chhipa's due process rights. As explained above, due process requires that criminal defendants have a meaningful opportunity to suppress the fruits of illegally acquired evidence. *See also Jencks v. United States*, 353 U.S. 657, 671 (1957) (the government cannot invoke its privileges to "deprive the accused of anything which might be material to his defense"); *Keith*, 407 U.S. at 318-24 (compelling disclosure of surveillance transcripts in a national security case); *Alderman*, 394 U.S. at 180-88 (same). Notice of surveillance was not only material to Mr. Chhipa's defense—it was indispensable. To effectively seek suppression, Mr. Chhipa must, at a minimum, be aware of all the surveillance that contributed to the government's investigation. As the PLCOB explained, "However, when the Board inquired, the government responded that it does not track how many times it has used Section 702 information that was identified through a U.S. person query as part of a criminal investigation or prosecution, and the government was unable to identify any instance in which this has occurred. Thus, U.S. persons have been unable to

challenge the use of evidence in criminal proceedings that was identified through U.S. person queries." PCLOB 2023 Report at 188.[35]

Yet courts have long found that notice is a constitutionally required element of surreptitious searches like wiretaps and sneak-and-peek entries. *See Berger*, 388 U.S. at 60 (finding wiretapping statute unconstitutional because, among other things, it had "no requirement for notice"); *Dalia*, 441 U.S. 238, 247- 48 (Title III provides "a constitutionally adequate substitute for advance notice" by requiring notice after the surveillance is completed (emphasis added)); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (finding sneak-and-peek warrant constitutionally defective for its failure to provide notice within a reasonable time). As the PCLOB explained,

> [I]n multiple cases, rather than providing notice to criminal defendants of Section 702-derived information, the government has instead sought to develop evidence through other sources without any reliance on FISA-obtained or -derived information. The lack of notice regarding use at early stages of investigations as well as the practice of relying on alternative sources of evidence even where Section 702 has been used in an investigation create risks that information derived from FISA may still affect the course of any investigation.

---

[35] The 2023 Report included the following footnote to its statement: "As of the 2020 certification of the Section 702 program, the FISC noted that the government had asserted that, based upon mandatory FISA training, FBI personnel 'should be aware' of the requirement to obtain an order from the FISC for such queries subject to Section 702(f)(2), and yet the FBI has not complied with this requirement. Memorandum Opinion and Order, at 48, *In re DNI/AG 702(h) Certification 2020-A and its Predecessor Certifications*, Docket No. 702(j)-20-01 and predecessor dockets, *In re DNI/AG 702(h) Certification 2020-B and its Predecessor Certifications*, Docket No. 702(j)-20-02 and predecessor dockets, *In re DNI/AG 702(h) Certification 2020-C and its Predecessor Certifications*, Docket No. 702(j)-20-03 and predecessor dockets (FISA Ct. Nov. 18, 2020).

PCLOB 2023 Report at 181. The PCOLB went on to state that "although we have no reason to doubt that the government has complied with its statutory notice obligations, and we recognize that the government chooses to rely on alternative sources of evidence in contexts beyond Section 702 to avoid disclosing sources and methods, these practices can prevent criminal defendants from learning about or being able to challenge evidence obtained through Section 702." *Id.*

In this case, there is a glaring hole in the information as to how the FBI would have even known about one particular email address. Without this information, Mr. Chhipa is unable to challenge the unreasonable intrusion, as well as the others about which he remains in the dark.

ii. 18 U.S.C. § 3504 and the Federal Rules entitle Mr. Chhipa to notice of the government's surveillance techniques.

Recognizing the dangers of surreptitious surveillance, Congress also provided a right to notice of surveillance by statute. Under 18 U.S.C. § 3504(a), if a party in a proceeding before any court claims that "evidence is inadmissible" because "it is the primary product of an unlawful act or because it was obtained by the exploitation of any unlawful act," then the government must "affirm or deny the occurrence of the alleged unlawful act." The statute defines "unlawful act" as "the use of any electronic, mechanical, or other device" in violation of the law. *Id.* § 3504(b). Thus, Section 3504 requires "the affirmance or denial of the fact of electronic surveillance, even if the government believes it was lawful." Kris & Wilson, 2 *National Security Investigations & Prosecutions* § 27:12 (2d ed. 2012).

A "cognizable claim" for notice under the statute "need be no more than a 'mere assertion'" that illegal surveillance has taken place. *United States v. Apple*, 915 F.2d 899, 905 (4th Cir. 1990) (citation omitted). The party must make a *prima facie* showing that he was "aggrieved" by the surveillance, which need only have a "colorable basis." *Id*. Mr. Chhipa has made such a showing with respect to several different types of surveillance, and especially Section 702. *See supra* Part II §D. For these reasons, Section 3504 requires notice of the surveillance methods used in this case.

Moreover, the Federal Rules of Criminal Procedure also support Mr. Chhipa's request for notice. Under Rule 16(a)(1)(B), Mr. Chhipa is expressly entitled to discovery of his relevant recorded statements. And under Rule 16(a)(1)(E), Mr. Chhipa is entitled to items "obtained from or belong[ing] to" him, as well as information "material to preparing the defense." See *id*. Because notice of the government's surveillance techniques is essential to Mr. Chhipa's ability to seek suppression, this information is plainly "material" under Rule 16(a)(1)(E)(i). *See United States v. Soto-Zuniga*, 837 F.3d 992, 1000-01 (9th Cir. 2016).

D. The government's use of CIPA to conceal surveillance of Mr. Chhipa violates both CIPA and due process

The government's *ex parte* submission of a CIPA Section 4 filing renders its contents unknown by defense counsel. It is likely, based on the facts of this investigation as well as one of DOJ's own IG reports, that the government's *ex parte* CIPA filing contains information regarding some or all of the surveillance techniques used to gather Mr. Chhipa's information. *See* DOJ Office of the Inspector

General, *A Review of the Department of Justice's Involvement with the President's Surveillance Program* (July 2009) ("OIG Report"). To the extent that the government concealed, is concealing, or will conceal surveillance techniques through CIPA, 18 U.S.C. app. III, it violates both CIPA and due process both of which require adversarial litigation of Fourth Amendment suppression issues—especially in cases involving complex surveillance.

CIPA's fundamental purpose is to regulate the discovery and use of classified information in a way that does not impair the defendant's right to due process. Under Section 4 of CIPA, courts apply a three-step procedure to determine whether classified, arguably discoverable information must be disclosed to the defense. They determine whether the material is (1) discoverable under the ordinary rules of criminal discovery; (2) in fact privileged; and (3) "at least helpful to the defense." *United States v. Hanna*, 661 F.3d 271, 295 (6th Cir. 2011). If the court concludes that the material is at least helpful, then it must be disclosed, though the court may impose conditions to safeguard sensitive information. *See United States v. Rezaq*, 134 F.3d 1121, 1142-43 (D.C. Cir. 1998).

As discussed throughout this motion, information concerning the government's surveillance of Mr. Chhipa in its investigation is plainly relevant and helpful, and should be disclosed to the defense. This information is discoverable, relevant, and helpful because it is a necessary predicate to any motion to suppress the government's evidence as fruit of an unlawful search. *See, e.g., United States v. Chun*, 503 F.2d 533, 536-37 & n.6 (9th Cir. 1974); *United States v. Aref*, 533 F.3d 72,

80 (2d Cir. 2008) (information is "helpful or material" if it is "useful to counter the government's case or to bolster a defense," and need not be "'favorable' in the *Brady* sense").

CIPA "does not expand or restrict established principles of discovery," *Sedaghaty*, 728 F.3d at 903—including Mr. Chhipa's rights to disclosure. Nor does due process permit the government to litigate Fourth Amendment suppression issues entirely in secret under the guise of "relevance." As the Supreme Court has made clear, Fourth Amendment suppression questions are notoriously fact-specific and complex—and must be resolved through disclosure and adversarial litigation. *See infra* Part III §E.

In its effort to withhold surveillance evidence under CIPA, the government may have advanced a number of arguments addressing fundamental Fourth Amendment issues. For example, as the OIG Report suggests, it may have argued that: (1) the surveillance was "too attenuated" from the trial evidence; (2) the surveillance was merely a "tip" or a "lead"; (3) the FISA applications broke the causal chain; (4) the trial evidence was obtained from an "independent" source; or (5) the "inevitable discovery" exception applied. Regardless of which theories the government advances in secret, using CIPA proceedings to withhold basic information about the surveillance of Mr. Chhipa—information relevant and helpful to a motion to suppress – violates due process and CIPA. This Court should require notice of all government surveillance used to collect Mr. Chhipa's information.

Because Mr. Chhipa does not have access to the *ex parte* record, he does not know where in that record the government's surveillance techniques are addressed. But to facilitate the review required in this case, the Court should begin with a complete and accurate picture of the surveillance actually used in this case. Accordingly, Mr. Chhipa respectfully requests that the Court: (1) Direct the government to identify the portions of the *ex parte* record addressing the government's surveillance of Mr. Chhipa; (2) Closely review the government's FISA applications to identify which surveillance techniques contributed to them; and (3) Require the government to identify, with specificity, the various types of surveillance that agents used in their investigation of Mr. Chhipa including how agents obtained the communications of his that the government withheld in discovery.[36] Following this review, the Court should order disclosure to defense counsel, under appropriate security measures, of the surveillance techniques agents used in their investigation; the legal authorities they relied upon; and the nature and volume of data collected.

E. *Ex Parte* proceedings to address this motion are antithetical to the adversary legal system

[36] Clarity as to the surveillance techniques actually used is essential, given reports that controversial techniques may be omitted, obscured, or vaguely described in court filings. *See* John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, http://reut.rs/1h07Hkl; Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, Wash. Post, Feb. 22, 2015, https://wapo.st/1K7cKfX.

Lack of disclosure renders the proceedings on the validity of the FISA electronic surveillance *ex parte*, as the challenges on Mr. Chhipa's behalf are made without access to documents and information essential to the determination of his motion. Such *ex parte* proceedings are antithetical to the adversary system that is the hallmark of American criminal justice.

As an initial matter, the adversary nature of our system of criminal justice warrants participation by the defense in the actual conversation regarding the legality of surveillance used to prosecute the defendants. Indeed, "Article III of the Constitution limits federal-court jurisdiction to 'Cases' and 'Controversies.' Those two words confine 'the business of federal courts to questions presented in an adversary context and in a form historically viewed as capable of resolution through the judicial process.'" *Massachusetts v. E.P.A.*, 549 U.S. 497, 516 (2007)(quoting *Flast v. Cohen*, 392 U.S. 83, 95 (1968)). Although proceedings to obtain judicial authorization for searches and surveillance by law enforcement are an exception to this rule, challenges to such proceedings and the resulting searches and surveillance are not.

As the Supreme Court has recognized, "'[f]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights. No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.'" *United States v. James Daniel Good Real Property, et. al.*, 510 U.S. 43, at 55 (1993) (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J.,

concurring). *See also United States v. Madori*, 419 F.3d 159, 171 (2d Cir. 2005) (citing *United States v. Arroyo-Angulo*, 580 F.2d at 1145 (closed proceedings "are fraught with the potential of abuse and, absent compelling necessity, must be avoided") (other citations omitted)).[37]

Indeed, "[f]or more than a century the central meaning of procedural due process has been clear: 'Parties whose rights are to be affected are entitled to be heard; and in order that they may enjoy that right they must first be notified.' It is equally fundamental that the right to notice and an opportunity to be heard 'must be granted at a meaningful time and in a meaningful manner.'" *Fuentes v. Shevin*, 407 U.S. 67, 80 (1972) (quoting *Baldwin v. Hale*, 1 Wall. 223, 233, 17 L.Ed. 531 (1864)).

In *United States v. Abuhamra*, 389 F.3d 309 (2d Cir. 2004), the Second Circuit reemphasized the importance of open, adversary proceedings, declaring that "[p]articularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other." 389 F.3d at 322-23 (citing *McGrath*, 341 U.S. at 171 n. 17 (Frankfurter, J., concurring)), which noted that "the duty lying upon every one who decides anything to act in good faith and fairly listen to both sides . . . always giving a fair opportunity to those who are parties in the controversy for correcting or

---

[37] Conversely, as Judge Learned Hand said in *United States v. Coplon*, 185 F.2d 629, 638 (2d Cir. 1950), cert. denied, 342 U.S. 920 (1952),"[f]ew weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which is seeks to forfeit the liberty of its citizens."

contradicting any relevant statement prejudicial to their view") (citation and internal quotation marks omitted).

As the Ninth Circuit observed in the closely analogous context of a secret evidence case, "'[o]ne would be hard pressed to design a procedure more likely to result in erroneous deprivations.' . . . [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error." *American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1069 (9th Cir. 1995) (quoting District Court); *see, e.g., id*. at 1070 (noting "enormous risk of error" in use of secret evidence).

Because Fifth Amendment due process protections apply in the pre-trial suppression context, circuit courts have held that the government must disclose information to a defendant that could affect the outcome of a suppression hearing. *See, e.g., United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) ("The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different."); *Smith v. Black*, 904 F.2d 950, 965-66 (5th Cir. 1990), vacated on other grounds, 503 U.S. 930 (1992) (due process mandates the disclosure of information in the government's possession if nondisclosure would "affect[] the outcome of [a] suppression hearing"). In other words, due process entitles defendants—at a minimum—to information that is relevant and helpful to their arguments that evidence was obtained illegally and should be suppressed. *See Roviaro v. United*

*State*s, 353 U.S. 53, 60 (1957). In these cases, disclosure under appropriate security measures is "necessary" for "an accurate determination of the legality" of the surveillance, 50 U.S.C. §§ 1806(f), 1825(g), and it is also necessary as a matter of constitutional right.

Similarly, in the Fourth Amendment context, including in relationship to electronic surveillance, the Supreme Court has twice rejected the use of *ex parte* proceedings on grounds that apply equally here. In *Alderman v. United States*, 394 U.S. 165 (1969), the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to the prosecution case against the defendants. The Court rejected the government's suggestion that the district court make that determination *in camera* and/or *ex parte*. The Court observed that

> An apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

Id. at 182.

In ordering disclosure of improperly recorded conversations, the Court declared:

> Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny that the Fourth Amendment exclusionary rule demands.

Id. at 184.

Likewise, the Court held in *Franks v. Delaware*, 438 U.S. 154 (1978), that a defendant, upon a preliminary showing of an intentional or reckless material falsehood in an affidavit underlying a search warrant, must be permitted to attack the veracity of that affidavit. The Court rested its decision in significant part on the inherent inadequacies of the *ex parte* nature of the procedure for issuing a search warrant, and the contrasting enhanced value of adversarial proceedings:

> The hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily ex parte, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an ex parte inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

438 U.S. at 169.

Franks holds that that criminal defendants are entitled to an evidentiary hearing upon a "substantial preliminary showing" that a warrant affidavit includes a knowing or reckless false statement. *Id*. at 155-56. But as a practical matter, defendants like Mr. Chhipa will virtually never be able to make the "substantial preliminary showing" required by *Franks*, because they cannot identify falsehoods or omissions in FISA affidavits they have not seen. *See United States v. Daoud*, 755 F.3d 479, 485-86 (7th Cir. 2014) (Rovner, J., concurring) ("[T]he secrecy

shrouding the FISA process renders it impossible for a defendant to meaningfully obtain relief under *Franks*.").

The same considerations that the Supreme Court found compelling in *Alderman* and *Franks* militate against *ex parte* procedures in the FISA context. Indeed, the lack of any authentic adversary proceedings in FISA litigation more than likely accounts for the government's perfect record in defending FISA and FISA-generated evidence. After all, denying an adversary access to the facts constitutes an advantage as powerful and insurmountable as exists in litigation.

Adversarial proceedings have often been the only way that long-standing, systematic Fourth Amendment violations have come to light. In *Carpenter*, 138 S. Ct. at 2216-17, the Supreme Court recognized that individuals have a protected privacy interest in a new type of personal data: the cell-site location information generated by their mobile phones. The government for years insisted that the third-party doctrine foreclosed any Fourth Amendment challenge and repeatedly persuaded courts to approve the surveillance with less than a warrant. Citing technological advances, the Supreme Court ultimately ruled otherwise. It did so, however, only with the benefit of extensive adversarial briefing on the technical details of the surveillance and the Fourth Amendment implications. *See id*. at 2217-18. *Carpenter* would have been unthinkable without adequate notice and disclosure to the defendant. The same lesson emerges from the government's secret surveillance.

Similarly, in *Clapper*, 785 F.3d at 822-24, the Second Circuit held that the NSA's bulk collection of Americans' call records was illegal. Although the FISC had secretly approved the surveillance for years, the outcome was markedly different in the face of adversarial litigation. The Second Circuit concluded that the suspicionless collection of Americans' call records violated the terms of Section 215 itself. *Id*.

Even internal oversight – less than adversarial, but better than completely secret – has illuminated Fourth Amendment violations that would otherwise go undetected. "[M]ost of FBI's compliance incidents have been discovered through audits by oversight entities rather than through internal compliance review." PCLOB 2023 Report at 119; *see also id* at 144 ("The majority of FBI's compliance incidents were discovered by external overseers, i.e., DOJ and ODNI.").

Even as the FISC itself has acknowledged, for example, without adversarial proceedings, systematic executive branch misconduct – including submission of FISA applications with "erroneous statements" and "omissions of material facts" – went entirely undetected by the courts until the FISC directed that the Department of Justice review FISA applications and submit a report to the FISC. *See In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp.2d at 620-21, *rev'd on other grounds*, 310 F.3d 717 (FISCR 2002).

However, as discussed above, the complete deference now required of the courts toward the executive concerning FISA renders any such "in-depth oversight" and "expanded conception of minimization" entirely illusory. *Belfield*, 692 F.2d at

148 & n. 34. As a result, §§1806(f) & (g), and the disclosure they authorize, assume significantly greater meaning and importance in evaluating the validity of FISA applications and surveillance techniques. Also, as noted above, the defendants' counsel possess the requisite security clearance to view the material, thereby eliminating any justification for non-disclosure or any claim that such limited, safe disclosure poses any danger to national security. Insofar as the government does have a legitimate interest in maintaining the secrecy of particular materials, that interest can be accommodated through "appropriate security procedures and protective orders." 50 U.S.C. §§ 1806(f), 1825(g).

In sum, the Court's review *in camera* is not a substitute for defense counsel's participation. As the Supreme Court recognized in *Alderman*, "[i]n our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate." 394 U.S. at 184. Accordingly, under §1806(f), §1806(g), and/or the Due Process clause, disclosure of the FISA and FAA materials and notice of all surveillance techniques is authorized and appropriate in this case.

CONCLUSION

For all of the above reasons, this Honorable Court should: suppress all interceptions made and electronic surveillance and physical searches conducted under FISA and the FAA and any fruits thereof; order the disclosure of the underlying FISA and FAA material, including the data, applications, and queries;

and compel the government to provide notice of all government surveillance programs used in the course of collecting Mr. Chhippa's information.

Respectfully Submitted,
MOHAMMED CHHIPA,
By Counsel

/s/

Jessica N. Carmichael, VSB #78339
Zachary A. Deubler, VSB #90669
CARMICHAEL ELLIS & BROCK, PLLC
108 N. Alfred Street, 1st Floor
Alexandria, VA 22314
703.684.7908 (T)
703.649.6360 (F)
zach@carmichaellegal.com
jessica@carmichaellegal.com

CERTIFICATE OF SERVICE

I hereby certify that on this 3rd day of June, 2024, I filed the foregoing pleading through the ECF system, which shall then send an electronic copy of this pleading to all parties in this action.

/s/
Jessica N. Carmichael